University of Wollongong

# Research Online

University of Wollongong Thesis Collection 1954-2016

University of Wollongong Thesis Collections

2005

# Applying wireless and mobile agent technologies for human decision making in the mission critical emergency environments

Hamidreza Pousti
*University of Wollongong*

# Applying wireless and mobile agent technologies for human decision making in the mission critical emergency environments

A thesis submitted in fulfilment of the
requirements for the award of the degree

Master of Information Systems (Research)

from

UNIVERSITY OF WOLLONGONG

by

Hamidreza Pousti
BSc (University of Tehran)
MICT (University of Wollongong)

School of Economics and Information Systems

2005

## Abstract

Emergency response tasks, both military and civilian, occur in what are termed, 'Extreme Environments' characterised by uncertainty, high stress physical situations, and time sensitive decision-making. Emergency response crews in such environments need to be highly mobile, utilising a variety of advanced wireless technologies to communicate while accomplishing their assignments. It is crucial for the users in the field to be aware of their own situation and the situation in their vicinity to construct their own goals in coping with unpredictable conditions. These are problems identified in the Small Unit Operation (SUO) model used by the military in situations where people and equipment work together to meet some mission objective. These entities may have distinct roles and information needs, and are often geographically distributed. Moreover, other groups of users in the command and control (C2) position need to have an overall and clear picture of the current state of the operation, at the necessary level of detail, in order to make the proper decisions based upon different types of information they receive and their own knowledge.

To tackle these issues, users face challenges concerned with the responsible for handling data through volatile wireless network connections and narrow bandwidth conditions. These conditions pose new challenges for all parties of users in terms of situation-awareness, sensemaking, reliable decision making and consequent actions.

The aim of this research is to focus on technologies that can help decision makers in two ways: reduce the level of environmental uncertainty, and provide better situation awareness and sensemaking for individuals and teams in extreme environments. These technologies are studied in the light of human sensemaking requirements and the factors contributing to human cognitive states, especially in time critical situations.

To achieve this aim, a secondary case study was carried out to identify various user requirements in dynamic environments, and the ways technologies can address those needs. Results show that many new wireless technologies, such as those based on Ultra Wideband (UWB) radio, demonstrate considerable potential for emergency response tasks circumstances. Furthermore, software agents show potential for deployment in emergency tasks to reduce the degree of uncertainty. Software mobile agents also show potential to improve the accuracy and agility of operations along with the ability to deal with the volatile wireless networks. The way decision makers understand their environmental states is vital for the success of emergency response operations. This understanding depends on the human capabilities of interpretation of information, as well as the memory and knowledge of decision makers at the moment the information is received. Thus, human issues need to be understood alongside the advances in technology. The potential contributions of the concept of mobile agents in this area is significant, especially where software mobile agents work as autonomous entities in order to handle the task and local decisions, on behalf of mobile emergency response crews.

These findings draw attention to the significant role of software mobile agents working in a meshed wireless network. They could provide an ubiquitous network in an extreme environment. They also have the capability of supporting users' situation awareness, sensemaking and critical decision making, vital in emergency response environments.

CERTIFICATION

I, Hamidreza Pousti, declare that this thesis, submitted in fulfilment of the requirements for the award of Master degree, in the Department of information systems, University of Wollongong, is wholly my own work unless otherwise referenced or acknowledged. The document has not been submitted for qualifications at any other academic institution.

Hamidreza. Pousti

03 August 2005

# Acknowledgements

Many people supported me during the completion of this thesis with criticism, helpful assistance, and references. This thesis would have never been possible without them. I would like to take this opportunity to offer thanks to all of them.

Firstly, my sincere thanks go to my supervisors, Associated Professor Helen Hasan and Professor Eryk Dutkiewicz. They have asked just the right questions at precisely the right times. They forced me to think when I believed I had thought enough. They gave strength to my mind, and they were always there. Helen, your time, patience and wisdom are greatly appreciated. Your earnest and steadfast mentorship helped reveal to me the true nature of scientific enquiry, for which you have earned my deepest respect and gratitude.  Also I am extremely grateful to Eryk for accepting the responsibility of being my co-supervisor. Eryk, you always steered me in the right direction when I wasn't certain which path to investigate and I acknowledge your awesome helps and contribution to my Master studies.

Many thanks to the University of Wollongong, particularly Department of Information Systems and the head of the department, Professor Peter Eklund, for supporting my research and giving me the chance to present my research topic there and providing me with valuable feedbacks. Likewise, I am grateful to the Faculty of Commerce at the University of Wollongong, especially Dean of Faculty of Commerce, Professor John Glynn and faculty's Research Manager, Mr. David Aylward, for supporting and providing me with amazing and unique facilities at the new Commerce Research Centre.

I owe a considerable dept of gratefulness to many friends and colleagues who filled my life with laughter and joy throughout my Master thesis.

I owe an immense debt of gratitude to my family and my acknowledgements now move closer to home to all my immediate and extended family. Mum and Dad, there are no word to express my gratitude but know it was you who have been my strength throughout. Dad (Pedaram) I am proud of you and I have had always this feeling in my heart for every single moment. Dad, your continual interest, advises, enthusiasm and support were my life-raft. Mum (Madaram) I learned the biggest lessens of my life in your hug. I understood what the love is just because of you. Your love and encouragement is my wealth.

And finally, my beloved wife, Naghmeh, for your unconditional love and support particularly, during the times when it all seemed too hard. You are more deserving of my thanks than anyone for bringing this thesis to end. Few people are as fortunate as I am, however, to have a spouse who has offered not only emotional support but intellectual support as well. Thank you for all your patience and scarifies you made in all countless nights and weekends I spent locked away in front of computer. This journey would not have been possible and such an amazing experience without you. I would like to thank you for, quite simply, everything: Naghmeh, your companionship means the world to me.

# Publications and Awards

- Pousti, H. and Hasan, H. (2005), ‘Knowledge Management through Mobile Networks in Emergency Situations’, Proceeding of 4th International Conference on Mobile Business, ICMB 2005, Sydney, Australia.

- Pousti, H., Hasan, H. and Dutkiewicz, E. (2005), ‘Application of Mobile Agents in Wireless-Based Mission Critical Emergency Operations’, Proceeding of the 11th International Conference on Distributed Multimedia Systems, DMS'2005, Banff, Canada.

- Pousti H. and Dutkiewicz, E. (2005),’ Effects of wireless-based mobile agents on the effectiveness of critical operations in extreme environments’, Accepted paper in the 2nd International conference on Mobile Technology, Applications and Systems, IEE Mobility 2005, Nov. 2005, Guangzhou, China.

- Selected thesis topic from the Faculty of Commerce for the PhD Research Commercialisation Workshop in Queensland, April 2005

# Table of Contents

## List of Figures

## List of Tables

## List of Abbreviations

# List of Figures

# List of Tables

# List of Abbreviations

| | |
|---|---|
| 3D | 3 Dimensions |
| APRL | Any-Path Routing without Loops |
| AWICS | Aircraft Wireless Intercommunications System |
| C2 | Command and Control |
| DARPA | Defense Advanced Research Projects Agency |
| EMS | Emergency Medical Service |
| FDNY | Fire Department of New York |
| FFD | Full Function Device |
| GPSR | Greedy Perimeter Stateless Routing |
| ICT | Information and Communications Technology |
| IEEE | Institute of Electrical and Electronics Engineers |
| IS | Information Systems |
| KM | Knowledge Management |
| LAN | Local Area Network |
| LPD | Low Probability of Detection |
| MANET | Mobile Ad hoc Network |
| M-MPR | Meshed Multi Path Routing |
| MP-MP | Multi Point to Multi Point |
| NYPD | New York Police Department |
| OFDM | Orthogonal Frequency Division Multiplexing |
| PAN | Personal Area Network |
| PAPD | Port Authority Police Department |
| PDA | Personal Digital Assistant |
| PHY/MAC | Physical/Media Access |
| PMP | Point to Multi Point |
| P-MP | Point to Multi Point |
| RAM | Random Access Memory |
| RETSINA | Reusable Environment for Task Structured Intelligent Network Agents |
| RF | Radio Frequency |
| RFD | Reduced Function Device |
| ROM | Read Only Memory |
| RPC | Remote Procedure Call |
| SA | Situation Awareness |
| SEA | Spokesman Election Algorithm |
| SUO | Small Unit Operation |
| TCP/IP | Transmission Control Protocol / Internet Protocol |
| UWB | Ultra Wide Band |
| WBAN | Wireless Body Area Network |
| Wi-Fi | Wireless Fidelity |
| WLAN | Wireless Local Area Network |
| WPAN | Wireless Personal Area Network |
| WSN | Wireless Sensor Network |
| WTC | World Trading Centre |

# Chapter 1

# Introduction

## 1.1 Background

In today's world, the coordination of multiple tasks in hazardous, uncertain, and time-stressed environments is becoming increasingly challenging, yet a vital concern for those responsible for public safety. Critical events of natural and man-made disasters-for example, earthquakes, tsunamis, environmental cleanup operations, and civilian and military crises, involve coordinated efforts by skilled personnel from different organisations such as fire fighters, police, and medical assistance personnel. These organisations need to cooperate in order to save lives, protect structural infrastructure and property, and evacuate victims to safety. They have to work together in hostile environments that are inherently diverse in terms of infrastructure where victims and rescuers are distributed across extended locations. In addition, these environments change unpredictably; for example, buildings and other infrastructure elements could collapse, blocking entrances, or fires could start, etc. In these situations, making timely decisions in order to act as quickly and effectively as possible is crucial for saving lives.

In such environments, human rescuers must communicate to make quick decisions under stress, and get victims to safety often at the price of risking their own life. They must have timely and accurate information regarding all parts of the disaster area, expected arrival times for additional resources, such as medical supplies and additional personnel, and they must coordinate the allocation of resources and instigation of new rescue activities. One of their main difficulties is that communications may be intermittent or non-existent. Hence partial and incomplete information is the norm rather than the exception.

Traditionally, in a disaster relief operation, the rescue workers communicate face to face, via telephones, mobile handsets or walkie-talkies. The gathering of required information is performed manually, or through searches in identified databases. These manual operations are inadequate to meet the urgent high-risk challenges of an emergency response on a large-scale.

Previous studies (Commtech ,2003; Marstrander, A. & Hanssen, B.I. 2002; Payne et al., 2000) show that main emergency challenges of first respondents to a large-scale disaster situation fall in three main categories. First, people can make inaccurate or even wrong decisions under the emotional stress of the situation and the cognitive overload caused by the large amounts of information that comes to them. The second category concerns about the relevant information that may not get accessed by the rescue workers whose operations depend on the field information. This problem is profound when information is slowly integrated and distributed throughout the teams, and consequently becomes obsolete and useless, because information cannot respond well to the changes of the dynamic environment, and does not reflect the real environmental situation. The third category is rescuers risk their lives to get victims to safety and suffer from the lack of proper information, which is intended to help them to become aware about their operation environment, threads and resources.

Existences of theologies by which first responders will be able to make more accurate and timely decisions are indispensable.

Recently, interest has been growing around technologies that could overcome these problems. One of the most promising is the use of new wireless technologies such as Ultra-wideband (UWB) radio to provide a more reliable communication system. These technologies can support different network topologies such as mesh. Mesh and UWB have many attractive features, including rapid self-configuring and self-healing networks, and bandwidth secure radio communications (Poor, 2003; Artimi, 2003).

Other research (McGrath et al., 2001; Lange and Oshima, 1999) reveals that mobile software agents feature properties that should prove a helpful component for integrated responses to civilian and military crises in unpredictable, time sensitive environments. Mobile agents have many fascinating and promising attributes including autonomy, adaptability, and persistency. These attributes make them able to act independently in their environment, sense and interact with their environment and make decisions on behalf of the users.

Until now there has been a lack of studies that approach issues of disaster response in a way that integrates these technologies and also considers the human and organisational perspectives.  There are some studies on the new wireless technologies and some research about mobile agents, but there are no reports about the combination of these two technologies in the context of emergency response tasks, addressing the advantages and challenges of coupling the capabilities of mobile agents with new wireless technologies. Furthermore, the ways that these technologies could help humans to make proper decisions in extreme and time critical situations are unclear throughout the literature.

The purpose of this study is to investigate the contribution of mobile agents - as a new paradigm of information gathering, processing and dissemination - together with new wireless networks to support human situational awareness and sensemaking, leading to decisions and actions in critical events of public safety. For this, the study aims to address those issues by investigating the following question:

> *'How the particular attributes of mobile agents and capabilities of new wireless radio technologies can help decision makers to get a better understanding and knowledge of their environment, become more aware of their situation and make sense of the operations' conditions in order to make more precise and timely decisions in extreme situations?'*

To achieve this goal, this research adopts a case study approach to the research topic, which is the recommended method for finding proper answers to the 'how' questions (Yin, 2003). This study uses a secondary case study approach to the research question in order to find and apply the previous outcomes of other case studies in the context of this research. These results will be considered as the bottom line of situation analysis in order to find out the gaps and the areas where this research can make contributions.

## 1.2 Outline of the Thesis

This section presents an outline of the chapters that comprise this thesis and briefly describes their contents.

Chapter 2 provides a discussion about the different and alternative methodologies that can be applied in this research. It contains a critical review of different methodologies in terms of their advantages and disadvantages in order to find out which one suits to this research.

Chapter 3 includes a comprehensive review of literature about the related fields. The purpose of this chapter is to provide a deep insight on the strengths, weaknesses and the gaps that exist within the body of knowledge in this area. It comprises two sections. The first section of the literature review is devoted to studying the literature about the agents, and specifically, mobile agent technologies. The second section is concerned with the literature and issues around public safety, wireless technologies and other important related fields.

Chapter 4 makes a profound review of the fall of the World Trade Centre on September 11, 2001 as a case of an extreme environment. It aims to identify the critical reasons and key moments that ended up with many damages and fatalities, especially on the lives of first responders. Also, the purpose of this chapter is to identify the technical and technological hurdles which contributed in the human mistakes and unsound decisions. At the end of this chapter, there is a discussion on the potential benefits of using mobile agents and new wireless technologies in an extreme environment.

Chapter 5 has a detailed discussion of how mobile agents and wireless technologies can contribute to emergency first responders' tasks. It introduces the methods and frameworks by which mobile agents can augment human operations performance. Also, it introduces and recommends the Ultra-Wideband radio technology as a preferred wireless technology, which can cope properly with the emergency tasks environment. The last and important section of this chapter presents the concepts of human situational awareness and their sensemaking requirements. This section addresses the cognitive and sensemaking issues that decision makers may face when they need to make a timely decision in a dynamic environment. It establishes a meaningful relation between technology and human aspects of decision making in order to augment the effectiveness of their decisions.

Finally, chapter 6 concludes the thesis with a summary of the major results obtained in earlier chapters. A summary of related open research issues is also presented.

# Chapter 2

# Research Methodology

## 2.1 Chapter Overview

The purpose of this chapter is to explain and justify the qualitative case-study methodology selected as most appropriate for the research presented in this thesis. The first section of the chapter discusses the necessity of choosing an appropriate research methodology for a research project and then focuses on the main qualitative research methods recommended in the information systems (IS) research literature. Each method is investigated in terms of its suitability, advantages and disadvantages for this research before justifying the choice made for this study.

## 2.2 Introduction

Methodology is one of the most important aspects of a research journey. An appropriate methodology helps researchers to conduct their research activities to obtain reliable and verifiable results. The research described in this thesis is distinctive in two respects. Firstly, it concerns critical emergency situations, which are difficult to study first hand, and secondly, it covers a breadth of human, social and technological concepts that are critically important but not easily measurable. Its position within the range of types of research and its consequent methodology therefore need careful explanation.

According to Redi and Pasteur (2004), scientists are 'observant' in that they notice things in the world around them by sensing what is going on in the world and become curious about what is happening. This can and does include reading and studying what others have done in the past because scientific knowledge is cumulative. So the research by which the scientific knowledge is gained is also cumulative. Redi and Pasteur (2004) also describe that scientists build their works on the work of previous researchers by finding out what previous research has already been done in the field. Therefore science is a “process” where new things are being discovered and old, long-held theories are modified or replaced with better ones as more data and knowledge is accumulated.

The research described in this thesis brings together an understanding of the capability of new technologies with the social and human aspects of information and knowledge management in situations of critical public safety. It thus aims to contribute knowledge by synthesizing and integrating emerging knowledge, demonstrating how these apply in a specific case.

## 2.3 The Case for a Qualitative Research Approach

The validity and credibility of new findings poses a considerably challenging issue for researchers. In fact, research methods are vital processes of a research, which ensures that the research outcomes are valid. Myers (1997) expresses this point and the importance of the research method by clarifying that all research, whether quantitative or qualitative, is based on some underlying assumptions about what constitutes 'valid' research and which research methods are appropriate. In this sense, the first important step is to adopt a proper type of research method.

For the research of this thesis, there are strong reasons to adopt qualitative research methods. One reason for this adoption is the fact that this research tries to understand the advantages and disadvantages of proposed technologies in the ways that they can help humans make decisions more accurately in critical situations. So, descriptions and perceptions of these technologies and the ways people could use these technologies effectively are topics of this research.

This perspective makes qualitative research a good choice for this research since qualitative research is “descriptive” in that the researcher is interested in process, meaning, and understanding gained through words or pictures. Also, the process of qualitative research is 'inductive' in that the researcher builds abstractions, concepts, hypotheses, and theories from details (Creswell, 1994). Myers (1997) describes a qualitative research method as that which is designed to help researchers understand people, and the social and cultural contexts within which they live. Another reason that favours the choice of a qualitative research method research approach is the accuracy it gives of concepts and contextual data.  According to Kaplan and Maxwell (1994), the goal of understanding a phenomenon from the point of view of the participants and its particular social and institutional context is largely lost when textual data are quantified. All these reasons make qualitative research an appropriate option for conducting the research as described in this thesis.

Although Avison and Myers (1995) mention eleven different research methods that can be appropriate in the area of IS, Myers (1997) states that the four most recommended and popular qualitative methods in IS are action research, grounded theory, case study research and ethnography. Also, he states that qualitative data sources include observation and participant observation (fieldwork), interviews and questionnaires, documents and texts, and the researcher's impressions and reactions. Considering the above arguments, the following section will continue to investigate the four primary methods recommended by Myers (1997), in order to find out which is most suited to this research.

## 2.4 Ethnography

Ethnography is a research methodology applied to qualitative research projects, especially information systems research when the research purpose is rich description of the studied subject. As Myers (1999) states, in ethnographic research an ethnographer is required to spend a significant amount of time in the field and plunge him/herself in the life of people s/he studies and seeks to place the phenomena studied in their social and cultural context. Harvey and Myers (1995) approach this method from the information systems angle and describe ethnography as a well suited methodology for information systems researchers that provides them with rich insights into the human, social and organizational aspects of information systems along with their development and application.

An ethnographic approach can also contribute in a lot of qualitative research with many benefits and advantages. One of the most valuable aspects of ethnographic research is its depth. According to Myers (1999), ethnography is the most "in-depth", or "intensive" research method possible. He explains that in ethnography the researcher is in the field for an extended period of time and sees what people are doing as well as what they say they are doing. So, over time the researcher is able to gain an in-depth understanding of the people, the organization, and the broader context within which they work. This is what Graue (2005) describes as the unique characteristic of the ethnographer who goes beyond the reporting events and details of experience and works to explain how these represent the webs of meaning in which the subject of the research lives. Another reason for using ethnography is to study actual practices in real world situations that enable a researcher to study organizations as the complex social, cultural and political systems that they are (Harvey and Myers, 1995). So, these aspects of ethnography make it a powerful and attractive research method of qualitative research, especially for studies concerned with social phenomena and related fields.

Although those advantages of ethnography make it so appealing to many qualitative researchers, some considerable problems pose as serious obstacles to adopt this method. According to Myers (1999), one of the main disadvantages of ethnographic research is that it takes a lot longer than most other kinds of research. Doing ethnography takes a great deal of time since considerable time is needed to prepare the members of the organization for the acceptance of such an in-depth approach. Furthermore, much time is needed to gather data and carry out many levels of interpretive analysis. Another disadvantage is accounted by Harvey and Myers (1995). They explain that ethnographic research is not extensive since an ethnographer usually studies just the one organization or the one culture. In fact, ethnographic research leads to in-depth knowledge only of particular contexts and situations, and it suffers from the lack of "generalisability".

As far as this research area is concerned, looking carefully at the issues around ethnographic research, this methodology could not be adopted as the primary research method for this research since it is not fitted to the research requirements and restrictions. The settings which would suit the study would not be conducive to having a non-qualified participant for reasons of security or safety. In addition, this research is highly constrained by the limited time frame due to the fact that it is master degree research. So it is expected that ethnography will not lead the researcher to the appropriate results in a short period of time. In addition, generalizable results are highly desirable in this research, because it involves the area of public safety where results should show an acceptable degree of certainty in order to be potentially applicable to life sensitive tasks.

## 2.5 Action Research

Action research is an established qualitative research method in the social and many other sciences that has been used since the mid-twentieth century. Baskerville (1999) states that this method produces highly relevant research results because it is grounded in practical actions aimed at solving an immediate problem situation. O'Brien (1998) suggests a more succinct definition for action research: "Action research aims to contribute both to the practical concerns of people in an immediate problematic situation and to further the goals of social science simultaneously. Thus, there is a dual commitment in action research to study a system and concurrently to collaborate with members of the system in changing it in what is together regarded as a desirable direction. Accomplishing this twin goal requires the active collaboration of researcher and client, and thus it stresses the importance of co-learning as a primary aspect of the research process."

These definitions for action research show that this method involves the studying of a system in its operating place in order to look at the ways people interact with the system and react to changes. This is the point explained by Avison et al. (1999) as they state that in action research the emphasis is more on what practitioners do than on what they say they do.

Baskerville and Wood-Harper (1998) believe that the action research method fairly fits to the researchers' requirements in the discipline of Information Systems. They state that the discipline of IS seems to be a very appropriate field for the use of action research methods since Information Systems is a highly applied field, almost vocational in nature. Baskerville and Wood-Harper (1998) state that action research methods are highly clinical in nature, and place IS researchers in a ‘helping role’ within the organizations that are being studied. They emphasize that action research merges research and practice, thus producing exceedingly relevant research findings and such relevance is an important measure of the significance of IS research.

These characteristics of action research make it an interesting method to use in running qualitative research. Baskerville (1999) spells out that action research responds directly to the pronounced needs for relevance in information systems research and provides a rewarding experience for researchers who want to work closely with the practitioner community. However, action research still poses considerable challenges. One important issue of the action research method relates to its validity among the scholars as a scientific research method. Baskerville (1999) describes this issue by highlighting the point that although action research is a highly qualitative research method, it is parked solidly outside of valid positivist techniques. Its qualitative and interpretive foundations make its journal length articles difficult, and the lack of generally agreed upon criteria for evaluating action research further complicates the publication review process. These constraints make the approach a difficult choice for academics tied tightly into the journal system of scholarly communication.

Another issue discussed by Baskerville (1999) lies in the nature of the action research method. He states that the action research collaborative framework diminishes the researcher's ability to control the process and the outcomes of the research, and that the lack of control makes it difficult to apply action research as an instrument in an orchestrated research program. Avison et al. (1999) also point out another potential problem of action research that concerns the ethical aspect of the research. As they explain, researchers and practitioners working together in the action research context need to have a mutually acceptable ethical framework because successful action research is unlikely where there is conflict between researchers and practitioners or among practitioners themselves.

Following the problems mentioned above, Avison et al. (1999) emphasize that this method is not recommended for novice researchers and practitioners due to the lack of guidelines assisting them to understand and engage in action research studies in terms of design, process, presentation and criteria for evaluation. This issue could significantly impact this research since it is a master level research that most likely could not cope properly with this methodology. There is also another key feature of action research that makes it unsuitable for contribution to this research. As

Baskerville (1999) describes, the fundamental contention of a action researcher is that complex social processes can be studied best by introducing changes into these processes and observing the effects of these changes. In the context of this research this argument means that these proposed approaches (mobile agents and new wireless technologies) should be considered as the source of change. It would then be necessary to study practitioners' response to this change. Technically, this would be a precise way of studying this system through. But in reality the technology is not yet available for this purpose and this approach could be considered for future research.

## 2.6 Grounded Theory

Grounded Theory is mostly described in the literature as a research method in which the theory is developed from the data, rather than the other way around. That makes this an inductive approach, meaning that it moves from the specific to the more general. As Strauss and Corbin (1990) explain, grounded theory is the method that is inductively derived from the study of the phenomenon it represents. They also spell out that grounded theory is discovered, developed and provisionally verified through systematic data collection and analysis of data relevant to that phenomenon. Therefore, data collection, analysis and theory stand in mutual relationship with each other. According to Davidson (2002), the primary objective of grounded theory is to expand upon an explanation of a phenomenon by identifying the key elements of that phenomenon and then categorizing the relationships of those elements to the context and process of the experiment. In other words, the goal is to go from the specific point or issue to the general results without losing sight of what makes the subject of a study unique. This makes the ground theory a reliable method since it is built directly on data. Siegel and Mart (1995) emphasize on this point by explaining that grounded theory presents a theory which is substantiated by data from field notes and the research results provide an idea where the data came from, how the data was rendered and how concepts were integrated. These characteristics of grounded theory make it a significant method in running qualitative researches.

Despite the fact that the ground theory method is a promising method for the qualitative researches in many disciplines, there are considerable issues that need to be taken in to account for its adoption. One important issue relates to the sophisticated steps that should be taken in order to achieve the desirable results. This implies that a researcher should have an acceptable level of skills and experiences to cope properly with the method's procedures and steps. This issue is highlighted by Davidson (2002) when he describes that grounded theory is a painstakingly precise method of study that requires high levels of both experience and insight on the part of the researcher. Davidson concludes that "novice researchers should avoid this method of study until they have achieved the proper qualities needed to effectively implement the approach".

Another disadvantage of the grounded theory method is the inconsistent and even controversial approaches that have been adopted by different scholars in running this methodology. In this respect, Chamberlain's (1995) studies show that in spite of the highly structured way in which grounded theory is presented, considerable variation in epistemological viewpoints toward the approach can be found (Epistemology is a branch of philosophy that studies knowledge and issues of scientific methodology, Heylighen, 1993).

Looking carefully at challenges concerning grounded theory and considering the fact that this research is at a master's level, realistically it is inappropriate to follow this methodology as it requires a high level of experiences and research skills. Also it is believed by the author that grounded theory cannot be well applied to this research since the environment of the subject that is studied in this research is highly dynamic and it does not depends on a single or a dominant phenomenon.

## 2.7 Case Study

The case study is also an accepted method in qualitative research. It is a methodology used by researchers in a variety of disciplines. As Yin (2003) states, it is not a surprise that the case study has been adopted as a common research strategy in many disciplines such as psychology, sociology, engineering and so forth. It is also an important research strategy within IS since it has made a great contribution in this area (Myers 1999, Klein & Myers, 1997).

According to Eisenhardt (1989) the case study is a research strategy that focuses on understanding the dynamics present within a single setting. This definition presented by Eisenhardt makes it clear that case studies are involved with the dynamic factors of the subject. Each of these factors could affect the overall situation of a single setting. However, this definition cannot identify what exactly a case study is and where it is applicable. Kaplan & Duchon (1988), define a case study based upon the type of the topic to which it may apply: "the essence of a case study, the central tendency among all types of case study, is that it tries to illuminate a decision or set of decisions: why they were taken, how they were implemented, and with what results". Among all of the definitions, Yin (2003) provides the more complete definition of the case study method. He states that the case study is an empirical inquiry that investigates a contemporary phenomenon within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident. In other words, Yin believes that researchers would use the case study method because they deliberately wanted to cover contextual conditions, believing that those might be highly relevant to researchers' phenomenon of study.

Case studies could be used for many purposes, and it could be used in order to derive different kinds of results. Eisenhardt (1989) states that case studies can be used to accomplish various aims such as providing descriptions for phenomena, testing theories and generating theories. Yin (2003) spells out that the distinctive need for case studies arises out of the desire to understand complex phenomenon in their social context. Therefore, this method allows the investigator to retain the holistic and meaningful characteristics of real-life events such as managerial processes, event consequences and, so on.

Compared with other research methods, what makes the case study a useful method for qualitative research is the way that it poses to tackle its objectives. This positioning can be cleared in the early stage of research by the research question. Eisenhardt (1989) states that the rationale for defining the research question is the same as it is in hypothesis-testing research, where without a research focus, it is easy to become overwhelmed by the volume of data. Also Yin (2003) believes that the first and most important condition for differentiating among the various research methods is to identify the type of research question being asked. As Yin argues, generally "what" questions may either be exploratory or about prevalence, while "how" and "why" questions are likely to favour the use of case studies. Yin (2003) also believes that "how" and "why" questions are more explanatory and likely to lead to the use of the case studies research strategy since such questions deal with operational links needing to be traced over time, rather than mere frequencies or incidence.

It is worthy to mention that there are many overlaps between case study method and other research strategies. For example, there is no hard and fast distinction between case study research and ethnographic research; but the main difference between the two methods is the extent to which the researcher immerses himself or herself in the life of the social group under study (Myers 1999; Klein & Myers, 1997). Also Yin (2003) states that case studies and history research can overlap but the case study's unique strength is its ability to deal with a variety of evidence beyond what might be available to conventional historical studies. This implies that case studies could use the same resources and same approach as other methods – especially historical research - when their area of studies overlaps with each other.

Based upon the above information and evidences, the researcher believes that the case study method will be a proper methodology to apply to this research. Firstly, this research investigates and studies the potential applications of specific technologies in a socio-technical context. It aims to understand "how" these technologies would help humans to overcome some technical communications problems in an extreme situation. Also, it tries to determine "how" mobile agents and wireless technologies would assist decision makers in making proper decisions based on the pertinent information. That means that the research question is mainly concerned with the "how" question. In this sense, as Yin (2003) explained, a case study is a good choice to conduct this research.

Secondly, considering the limitations of this master level's research, time restrictions and research skills are the main obstacles in adopting other methodologies such as ethnography, action research and, grounded theory. A case study is a good option since it also overlaps with other research methods such as historical research that allows using a variety of resources like reports, documentaries, pictures and so on. This is a significant advantage to this research since it could alleviate the problem of evidence and data gathering in a short time frame.

In this research, a single comprehensive case study approach is used. According to Lee (1989), one important point in the case study method is the justifications of selecting the number of cases for one study. Lee (1989) spells out that the single-case analysis is justified when the case in question is a critical, extreme or unique case. This is what Yin (2003, p40) describes as the rationale of selecting a single-case study approach. He states that there are five rationales for doing a single-case study rather that choosing a multi-case study approach: critical, extreme/unique, representative/typical, revelatory and, longitudinal. Yin (2003) explains that in an extreme/unique case, rare or unusual situations would arise in a period of time, and accordingly specific, results would be gained which are not attainable in common and usual situations. In such circumstances, Yin believes that the single-case study is an appropriate research method.

## 2.9 Justification for the Case Study Used in this Research

Case studies can generate innovative new interpretations and concepts by selectively analyzing a single case (Tellis, 1997). Case studies can provide the means to generalize a theory as laboratory experiments lend themselves to low-level generalizations (Yin 2003). This approach allows for a broader explanation of how cases that are unexpected can provide insight into the application of the issue subject to study, in this case, the applications and implications of wireless technologies and mobile agents in the public safety domain .The frequent use of case studies is due to the fact that they allow close in-depth analysis and understanding of specific cases, aid in understanding unique realms of inquiry, and provide insight into cases that could not be duplicated experimentally. Relying on a single case is a useful way of study when there is enough evidence and documentation on it. Reason (1990) has stated that when sufficient evidence regarding a single case is available then, "we are able to study the interaction of the various causal factors over an extended time scale in a way that would be difficult to achieve by other means."

This leads the researcher described in this thesis to adopt a single-case approach, since it will investigate situations in a public safety operation where the circumstances are highly dynamic and the environment is extreme. As mentioned earlier, the main reason to adopt this approach is that case studies have provided an established, valuable method of the study of real situations where many different factors come into play. In this thesis, the application of wireless technology and mobile agents in the public safety domain and rescue operations is evaluated by examining a single case, a portion of the September 11 of 2001 World Trading Centre collapse. This is what would be described as a secondary case, as the primary data is not collected by the researcher himself, but relies on available accounts and documentation, which in this case is plentiful.

Secondary sources of research refers to any materials such as books, articles, documents, etc. which have been previously gathered and published. The option of using Media (press, movies, documentaries, etc.), is one of the most well-known sources of secondary data and it has been suggested by many scholars (Dunsmuir and Williams, 1991; Yin, 2003).

As Myers (1997) states, sometimes primary data collection simply is not necessary and secondary data may be available, entirely appropriate, wholly adequate to draw conclusions and answer the question or solve the problem. Nevertheless, secondary sources often prove to be of great value in exploratory research. In fact, investigating data that have been compiled for some purposes other than the project at hand is one of the most frequent forms of exploratory research and investigating such sources has saved many researchers from 'reinventing the wheel' in primary data collection. This is also a technique for both descriptive and conclusive research with great influences on the process of fact finding (Zikmund, 2000).

Generally, literature (Crawford, 1997; Dunsmuir and Williams, 1991; Zikmund, 2000) shows that there are many advantages in using secondary data in research since the secondary research data are:

- Cheap and accessible
- Often the only available resource (i.e. extreme cases)
- Only way to examine large-scale trends
- The time involved in searching secondary sources is much less than that needed to complete primary data collection

- It can play a substantial role in the exploratory phase of the research when the task at hand is to define the research problem and to generate hypotheses

Using the secondary data in the qualitative research can provide a useful ground for the qualitative sampling and case investigations. According to Liamputtong and Ezzy (2005), in some qualitative research, for example, 'Purposive sampling', the researcher uses secondary data and aims to select information-rich cases for in-depth studies to examine meanings, interpretations, processes and theory. Also they describe 'Extreme or deviant case sampling' as another base for secondary data usage in qualitative research, where cases are selected that are unusual or have distinctive characteristics and a researcher's aim is to elicit rich and detailed information that provides a new perspective on more typical cases.

Nevertheless, much literature (Crawford, 1997; Dunsmuir and Williams, 1991; Zikmund ,2000) reveals that there are also drawbacks in using secondary data, and that researchers should be cautious about them. Secondary research disadvantages are:

- Lack of consistency of perspective
- Biases and inaccuracies can not be checked
- The concern over whether any data can be totally separated from the context of its collection
- Secondary data may be outdated or may not exactly meet the needs of the researcher because they were collected for another purpose

Following the above arguments, we believe the term of the 'secondary case study' will fit the context and purpose of this research since it investigates an extreme incident. In fact, this case study allows for an evaluation of an extreme incident that could not be replicated by experimental means. Reason (1990) has a unique opinion about the relation between case studies and human made disasters. Reason (1990) states that case studies have taught that “disasters are very rarely the product of a single monumental blunder.” He further states that human-made disasters are generally the result of accumulating apparently negligible consequences that compound to contribute to the undesired result.

Two types of communications were selected for evaluation: inter-team communications and communications among teams and command and control units (C2 units). These are the most important forms of communications that would take place in incident rescue tasks, especially in a civilian fire situation (US Fire Department, 2003). The types of communications are under examination in this thesis, not the fire itself.

In the context of this thesis, there are many reasons that makes the September 11 WTC disaster an appropriate case to study. Among those reasons are:

1- The size of the event is quite huge by any measure. According to the centre of fire statistics of International Technical Committee for the Prevention and Extinction of Fire (CITF) (2003), on the September 11, 2001 the biggest number of firefighters' fatalities in the history of civilian rescue operations has occurred. So, the outcome results of the case study would be extended and applied to any other situations where public safety operations are subject to investigation. Therefore, studying the reasons that caused this significant number of casualties could be significant in any other situation.

2- Many reports and evidence reveal that there was considerable communications problems among individual firefighters and between commanders and their crew during the rescue operations. Communication problems had a significant impact on the overall rescue operations performance in the WTC rescue operation and on the cooperation among the parties involved in the rescue tasks. This case will significantly highlight these challenges.

3- This case will explicitly stress the crucial role of sharing vital information during the rescue operations in extreme environments. On September 11, many firefighters lost their lives since they didn’t receive the announced evacuation warnings. They seriously suffered from the lack of vital information during the rescue operation, especially when the towers started to collapse. Consequently, this had a direct impact on the number of firefighter fatalities.

4- Traditional communication systems showed significant problems in the WTC disaster. They showed that it is hard to rely on those systems, particularly where the situation and environment are under extreme pressure and time is a critical factor in making decisions.

5- It highlights that it is important to have a reliable and flexible communication network which could work in a situation where physical and communication infrastructure have vanished. Thus, it can connect users together, helping them to exchange the minimum amount of data vital to their operations.

6- The case of the WTC collapse shows that voice communication is essential but not sufficient for the users. Sensing the probable hazards when the environment is highly dynamic can also help them to become aware of the situation around them.

7- The WTC collapse reveals that critical decisions rely heavily on the manner in which information travels though the wireless network. It is critical to have mechanisms that can cope with wireless network disconnections, data communication interruptions and other challenges concerning the volatile nature of wireless networks.

8- So far, much research has been carried out regarding the September 11, 2001 WTC collapse; it has been studied from different points of view. However, to the best of my knowledge, the application of new wireless technologies and mobile agents has not been investigated in this context. Considering the unique significance of this case, this study could provide a better understanding of new applications, implications, advantages and disadvantages of these technologies, especially in situations of extreme environment rescue operations.

## 2.10 Limitations

Case studies can expand on principles that “can reasonably be expected to reduce either the occurrence of errors or their damaging consequences” (Reason 1990). The study of individual cases can provide understanding into the extent and scope of human and technology performance capabilities that laboratory environments could not follow. It would be impractical to attempt to replicate the extreme circumstances that model the real world in a laboratory environment. The ability to investigate and learn from these extremes in human and technology capabilities, high risk decision making processes, and problem solving under life threatening situations can only be studied in their complete context from case studies. This is one of the limitations concerning this case study.

Another limitation, according to Reason (1990), is the limited information that is available from past accident investigations and their reports, where the tendency of documentation is to be “digitized” as opposed to an original event. Real events are usually more complex and continuous due to the fact that the nature of events is “analog.” In fact, past accident reports lack the information that was potentially available since the broader, richer, and more complex possibilities of the original account can be compromised in the written form. This thesis is constrained by this limitation as well, since much of the evidence in the form of interviews, reports and documentaries is available in digital format, and information regarding the WTC collapse and its consequences is being revised and may be changed.

Drawing a conclusion from the material discussed in this chapter, it is believed that the case study is the best method suited to this research. The above discussion reveals that every recommended method in IS has its own advantages and problems. But an analogy between these methods in terms of their strengths and weaknesses shows that the case study is the one with more promise to lead this research into a reliable outcome.

Before any analysis of the case, it is essential to have a deep review of the relevant literature in order to summarise outcomes of previous research in the different areas of the topic, what is already known, gaps in that knowledge, and so forth. For this reason, the following chapter is devoted to the review of various literatures.

# Chapter 3

# Literature Review

## 3.1 Introduction

The literature review is a critical look at the existing research that is significant to the work of researcher. It is not just a summary, it is also vital for evaluating other people's work, show the relationships between different works, and show how they might relate to subject of research. Literature review should provide the context for the research by looking at what work has already been done in your research area. According to McKillap (2000) states, literature review is a very careful and critical evaluation of what everybody else has done in the field and possibly inside related fields in terms of your research. It is looking around the filed of other people's work and it is not just look at what people have done but also the researcher should try to be comprehensive as possible and should be very critical in order to identify strengths and weaknesses and most importantly the gaps in what has been done already.

The following section makes a comprehensive review of the related literature to this research. There are two different but related reviews of literature. The first review concerns the related literature in field of agents. It tried to identify the contribution of the agents in the area of uncertain environments and their strengths and weaknesses in this area. The second part will have a look and critical review on the topics of public safety, wireless technologies and related issues. This section will try to identify the key points of these areas in terms of their capabilities, weaknesses and future development in order to find out their direct and indirect contributions in this research.

## 3.2 Review of agent technology literature

### 3.2.1 Defining an agent

Agents are inspired by many diverse disciplines and draw on many different areas of research, such as computer science, psychology, philosophy and so forth. So, it is difficult to find a succinct definition for an agent that includes all the aspects that most researchers and developers consider an agent to be, and exclude all of the aspects they are not considered to be. The concept of an agent can be traced back to the early days of research into Distributed Artificial Intelligence in the 1970s and Carl Hewitt's concurrent Actor model (Hewitt C., Yonezawa, A., 1977). In this model, Hewitt proposed the concept of a self-contained, interactive and concurrently-executing object, which he called 'actor'. This object had encapsulated internal state and could respond to messages from other similar objects. It also had a mail address and some behaviour. Such objects had the ability to communicate with other objects by message-passing and they could carry out their actions concurrently.

So far, researchers involved in the agent technology studies have offered a variety of definitions, each hoping to explicate their own use of the word "agent". These definitions range from simple to of lengthy, complicated and demanding ones. Consequently, finding a proper general definition for the term "agent" has become an issue among researchers who work theoretically, or develop practical agent-based systems.

As Wooldridge and Jennings (1995) express, defining a universal agent is challenging, because there is no general agreement as to what constitutes an agent. The question "what is an agent?" is emblematic of agent-based research community. They believe that the source of this problem goes back to the widely used term “agent” by many people working in closely related areas. This defies attempts to produce a single, universally accepted definition. They also point out that if many people successfully develop interesting and useful applications for agents, then it hardly matters if there are not any agreements about trivial terminological details.

Other research such as that carried out by Franklin and Graesser (1996) show that finding a generic and precise definition for agent is a painful task that is unlikely to end up with desirable outcomes. They mention ten different definitions within different software systems as developed by distinct groups of researchers. The research shows that each group uses various approaches and emphasizes particular things in their definitions of agents. These disparities of definitions have led Franklin and Graesser (1996) to conclude that there is no general agreement of what an agent is or how agents differ from a software programs.

Other experts such as Russel and Norving (2003, p.32), the two outstanding researchers in the area of agent technologies have shown some other ideas about the definition of agents that seems more practical and simple. They generally define an agent as anything that can be viewed as perceiving its environment through the sensors, and acting upon that environment through actuators (Figure 3.1). Their agent could be a human, a robot, a piece of software or whatever else that could interact with its environment by sensing and acting upon its perception of the environment.

They clarify an agent in its simplest form as a reflex agent who selects actions on the basis of the current perception of its environment and the condition-action rules.

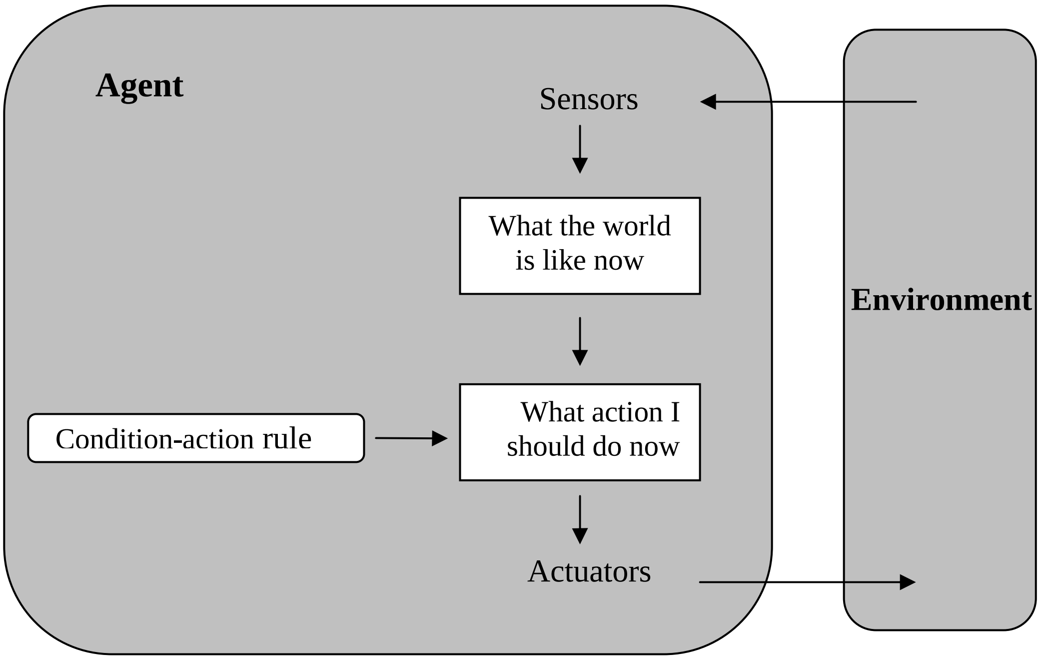


**Figure 3.1** Interactions between an agent and its environment (Russel & Norving, 2003)

There is no universal definition of an agent, and definitions can be made based upon the nature of the system an agent is designed for and its attributes. Wooldridge and Jennings (1995) explain this point by distinguishing the general usage of the term agent into two ideas. They state that the first notion of agency is a weak notion, which is relatively uncontentious. Using term of agent in this notion is to indicate a hardware or software-based computer system that enjoys four primary properties: autonomy, social ability, reactivity and pro-activeness. On the other hand, the second notion of agency is stronger and potentially more controversial. It has a more specific meaning that describes an agent as a computer system that in addition to having the four primary properties is either conceptualised or implemented using concepts that are more often applied to humans, such as knowledge, belief, and intention.

Other definitions such as the one expressed by Foner (1993; 1997) follows the same idea for defining an agent. Foner (1997) tends to define an agent by looking at its attributes and contributions in a specific system, such as their ability to collaborate with users to improve the accomplishment of the users' task.

Bradshaw (1998) believes that agenthood is difficult because one person's "intelligent agent" is another person's "smart object"; and today's "smart object" is tomorrow's "dumb program", and the key distinction is in people's expectations and their points of view. Bradshaw (1998) also argues that there is confusion in the concept of agents due to the many varieties that have been proliferated so far. Indeed, there has been an explosion in the use of the term without a corresponding consensus on what it means. However, Bradshaw has a more categorized notion of this issue as he explains the two distinct but related approaches to defining an agent: one based on the notion of agenthood as an ascription made by some person, the other based on a description of the attributes that (software) agents are designed to possess.

All of the different opinions about the definition of the term "agent" point to the common idea that defining any agent heavily relies on its attributes and characteristics subjected to study, and also on the environment it is situated (Franklin and Graesser, 1996; Shoham, 1997; Russel and Norving 2003). For example, Franklin and Graesser (1995) define their agent as "An autonomous entity which is a system situated within and part of an environment that senses that environment and acts on it, over time, in pursuit of its own agenda and so as to effect what it senses in the future". Shoham (1997) provide a definition of an agent (software agent) and Bradshaw (1998) claims that Shoham's definition is more acceptable among the researchers, that is: 'a software entity which functions continuously and autonomously in a particular environment, often inhabited by other agents and processes'.

These definitions show that it is worthwhile studying agents' attributes and their environment for a better understanding of the role of agents' characteristics and their environments in their definition.

### 3.2.2 Attributes and Characteristics of Agents

As it is mentioned in the previous section, there is no universal definition for the agents and they are mostly known by their dominant characteristics and major functionalities. For example, some agents are known as mobile agents, this implies that their most considerable characteristic is 'mobility' and this attribute is their dominant characteristics. Although, they still embrace their autonomy and persistency to accomplish their tasks.

Agents' attributes show the ways that agents can interact with their environment. This is an important issue when agents are applied to solve a particular problem in a particular environment. For this reason, studying the characteristics of agents helps the researchers to classify agents into different categories based upon how each agent class matches up with their ability to solve individual problems.

Bradshaw (1998) has carried out a comprehensive research which shows that the attributes of an agent derive from the designers' desire and goals. According to Bradshaw, an agent should be able to accomplish its activities in a flexible and intelligent manner and also be able to be responsive to changes in the environment without requiring constant human guidance or intervention.  Shoham (1997) define an agent as a software entity that functions continuously and autonomously in a particular environment, often inhabited by other agents and processes. Shoham's definition of an agent is a concise definition that attempts to institute a reasonable conjunction between attributes of every single agent and its operating environment, in which other agents might also operate. However, this definition does not provide any view of how agents can operate effectively in company of other agents to satisfy a particular goal. Despite of this, Bradshaw (1998) sticks with the Shoham's definition as an acceptable definition of an agent and then expresses that ideally an agent that functions continuously in an environment over a long period of time will learn from its experience. He also states that an agent inhabits an environment with other agents and processes. An agent should be able to communicate and cooperate with such agents and processes, and move from place to place to achieve its goals or solve a particular problem.

Consistent with the requirements of a particular problem, each agent might possess to a greater or lesser degree of attributes like the ones described by Wooldridge and Jennings (1995), Etzioni and Weld (1995) and Franklin and Graesser (1996) as follow:

- Autonomy: the ability to operate without the direct intervention of humans or other agents and have some kind of control over their actions and internal state.
- Reactivity: the ability to selectively sense and act.
- Collaborative behaviour: the ability to work in concert with other agents to achieve a common goal.

- Inferential capability: agents can act on abstract task specifications, using prior knowledge of general goals and preferred methods to achieve flexibility. This goes beyond the information given, and may have explicit models of self, user, situation, and/or other agents.
- Persistency: persistence of identity and state over long periods of time.
- Personality: the capability of manifesting the attributes of a 'believable' character such as emotion.
- Adaptivity and learning: being able to learn and improve with experience.
- Mobility: being able to migrate in a self-directed way from one host platform to another one.
- Pro-Activeness: do not simply act in response to their environment; they are able to exhibit goal-directed behaviour by taking the initiative
- Social Ability and knowledge-level communication ability: able to interact with other agents (and possibly humans) via some kind of agent-communication language and communication protocols.

Several in the agent research community have proposed various classification schemes and taxonomies (Franklin and Graesser, 1996) based on the agents' attributes. For instance, Artificial Intelligence researchers often distinguish between weak and strong notions of agency. Wooldridge and Jennings (1995) described and discussed these notions by emphasizing the point that agents of the latter variety are designed to possess explicit mentalistic or emotional qualities such as:

- Veracity that  is the assumption that an agent will not knowingly communicate false information

- Benevolence is the assumption that agents do not have conflicting goals, and that every agent will therefore always try to do what is asked of it
- Rationality is the assumption that an agent will act in order to achieve its goals, and will not act in such a way as to prevent its goals being achieved - at least insofar as its beliefs permit

Wooldridge and Jennings (1995) have a deeper view and described an agent as a system. Their system is most conveniently described by the intentional perspective which is represented by the information attitudes such as knowledge, belief and pro-attitudes such as desire, intention, obligation, commitment and so forth.

One important idea about the study of the agent attributes is their significant role in defining a new particular type or class of agent that can satisfy a specific goal. For instance, Nwana (1996), states that agents may be classified along several ideal and primary attributes, which agents should exhibit. The author describes that a combination of three minimal characteristics (Figure 3.2) can derive four types of different agents: collaborative agents, collaborative learning agents, interface agents and smart agents.

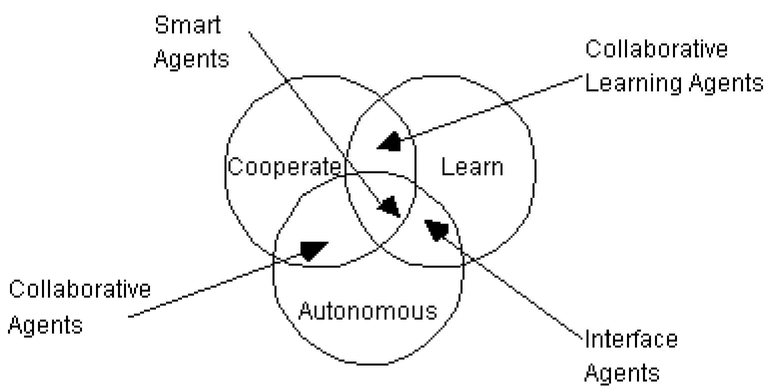


**Figure 3.2** Combination of primary attributes of agents (Nwana, 1996)

This literature shows that agents are mostly known by their attributes. This implies that agents' attributes identifies what a particular agent is and what it can do.

Among all the attributes, autonomy of an agent is an important characteristic that plays a centric role in any attempt for defining an agent (Wooldridge and Jennings, 1995; Franklin and Graesser 1996; Bradshaw, 1997; Shoham, 1997). Early research by Maes (1990) describes an autonomous agent and its architecture as the direct coupling of perception and action, in a distributed and decentralized fashion which dynamically interacts with the environment and holds essential mechanisms to cope with resource limitation and incomplete knowledge. As Shen and Norrie (1997) describe in their article, Maes's (1990) idea on autonomous agents is developed around three key notions: emergent functionality, agent task level decomposition and exploitation of reasoning methods. That each of these describes the level of required autonomy of an agent to accomplish its tasks.

There are different definitions in the research literature of autonomous agents. Shen and Norrie (1997) pick a more general definition that defines the autonomous agents as the computer systems or subsystems that are capable of independent action in dynamic, unpredictable environments. They state that only a few agent-based systems developed in the world can be considered as such autonomous agent systems and they argue that an autonomous agent should have at least have four characteristics: (1) it is not controlled or managed by any other software agents or human beings; (2) it can communicate/interact directly with any other agents in the system and other external systems ; (3) it has knowledge about other agents and their environment; (4) it has its own goals and an associated set of motivations.

One of the important features of autonomous agents is their independency (Shen, W. and Norrie, D. 1997). As Russell and Norving (2003) describe, the concept of autonomy form a more practical and designing point of view. An agent rationally should be autonomous so it can learn what it can do to compensate for partial or incorrect prior knowledge. Through a comparison between agents and animals with enough built-in reflexes such as a mouse, Russell and Norving (2003) argue that agents with some initial knowledge as well as the ability to learn can get sufficient experience of their environment and then become effectively independent of their prior knowledge, which was borrowed from their designer - and consequently behave more autonomously - in a vast variety of environments.

Luck and d'Inverno (2001) research points out that an autonomous agent may have its own goals and associated motivations. They describe this view by expressing an autonomous agent as an instantiation of an agent together with an associated set of motivations. Also Wooldridge and Jennings (1995) have a more goal-oriented approach to the concept of autonomy and they express the autonomy attribute of an agent as the capability of action in its environment in order to meet its design objectives.

These research and literature about the agents' autonomy makes an important point clear that agents can handle and perform tasks on behalf of users independently without any undesired interventions. Also they conclude that autonomy of agent helps the users to hand over some hard, dangerous or time consuming task to agents.

### 3.2.3 Agent Environment

Wooldridge (2001) and Russell and Norving (2003) have carried out some comprehensive and considerable research about the agents' environment. They state that the agents' task environments are essentially the "problems" to which agents are the "solutions". Russell and Norving (2003) suggested a classification of environment properties and divided the environment properties in six different groups:

1) Fully observable versus partially observable: According to Russell and Norving (2003) if an agent's sensor gives it access to the complete state of the environment at each point in time, then the environment task is fully observable and it is effectively fully observable if the sensors detect all the aspects that are relevant to the choice of action. An environment might be partially observable because of noisy inaccurate sensors or because parts of the state are simply missing from the sensor data.

2) Deterministic versus stochastic: A deterministic environment is one in which any action has a single guaranteed effect and there is no uncertainty about the state that will result from performing an action (Wooldridge, 2001). However, if the environment is complex then it could be partially observable and it could appear to be stochastic.

3) Episodic versus sequential: According to Russell and Norving (2003) in an episodic environment, the agent's experience is divided into episodes and the choice of action in each episode depends only on the episode itself and the current decision doesn't affect whether the next part is defective. However, in sequential environment the current decision could affect all future decisions.

4) Static versus dynamic: Russell and Norving (2003) define a static environment as one that can be assumed to remain unchanged except by the performance of action by agent. In contrast, a dynamic environment is one that has other processes operating on it and which hence changes in ways beyond the agent's control. As Wooldridge (2001) states, the physical world is a highly dynamic environment.

5) Discrete versus continuous: Russell and Norving (2003) express that a discrete/continuous distinction can be applied to the state of the environment, to the way time is handled, and to the percepts and actions of the agent. Wooldridge (2001) states than an environment is discrete if there are a fixed, finite number of actions and percepts in it, otherwise the environment is a continuous one.

6) Single agent versus multiagent: Russell and Norving (2003) point out that the distinction between single-agent and multiagent environments seems to be simple but in a multiagent environment the most considerable point is how agents interact with each other. They suggest four kind of interaction among agents in a multi agent environment: Competition, Communication, Cooperation, and Stochastic behaviour.

Wooldridge (2001) explains the role and contribution of each environmental characteristic in the agent design and its attributions. He also states that the most complex general class of environments are those that are partially visible (inaccessible), non-deterministic, dynamic, and continuous. As Hewitt (1986) states, environments that have these characteristics are often referred to as open environments. Also Russell and Norving (2003) indicate that most real situations are so complex that whether they are really deterministic is a debatable point.

The more interesting result that comes out of this literature is that agents' are able to adapt and operate in dynamic environments. As the literature shows, classes of agent environments fit the situation where is so dynamic and unpredictable. Agents show considerable potential to perform in such an environment.

### 3.2.4 Mobile Agents

A lot of research has focused on the mobile agents and their specifications. According to Wooldridge and Jennings (1995), Sundsted (1998), and Lange and Oshima (1999) mobility is one important characteristic of agents and it is an orthogonal property of agents, that is, not all agents are mobile.

Peramanu (2003) explains that the rapidly evolving network and computer technology, coupled with the exponential growth of the online services and available information, will soon bring us to the point where many people will have fast, pervasive access to a phenomenal amount of information from anywhere and everywhere. Hence, mobile agents will be an essential tool for allowing such access.
Kotz and Gray (1999) spell out how current technological trends may lead to a system based substantially on mobile agents. It seems likely that nearly all major systems and Internet sites will be capable of hosting and willing to host mobile agents.

'Mobile agents' is a contentious topic that has attracted some researchers and repelled others. White (1996) in his article about General Magic’s mobile agent system (Telescript) describes mobile agents as a new way of communication between hosts. Hosts not only call procedures in other hosts but also supply procedures to be performed on these hosts and consequently the ongoing interaction does not require ongoing communication. As White (1996) states, mobile agents provide an alternative method to the remote procedure calling (RPC) in which the procedure calls are remote rather than local and they requires the ongoing interaction for the ongoing communication. According to Milojicic (1999) the term “mobile agent” was introduced by Telescript, which supported mobility at the programming language level. In many ways telescript was ahead of time, including its support for mobile agents.

Liu (2004) describes a mobile agent as a “serializable object” that is an object whose data as well as state can be marshalled for transportation over the network. He introduces the basic architecture for supporting mobile agents and spells out that mobile agents carry the four essential data items: Identifying information, Itinerary, Task data and the Logic Code to perform its tasks. Liu (2004) also explains how a mobile agent travels from one host to another and make use of local resources to perform its task through the agent servers (Figure 3.3).

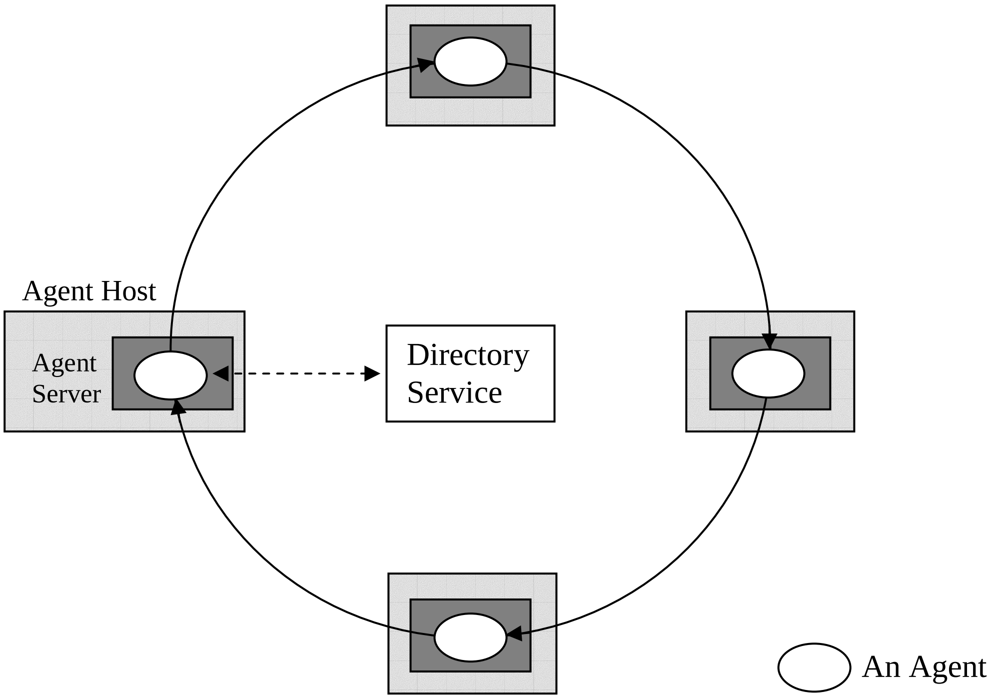


**Figure 3.3** The framework in which a mobile agent can move throughout a network (Liu, 2004)

Some authors such as Nwana and Azarmi (1997) classify mobile agents as a special type of agent. However, many others separate the agency from mobility as in Vitek and Tschudin (1997).

Pham and Karmouch (1998) also carried out some research about the mobile agent and its applications. They stated that the term 'mobile agent' contains two distinct concepts of mobility and agency and it refers simply to a self-contained and identifiable computer program that can move within the network and act on behalf of the user or another entity.

According to Milojicic(1999), mobile agents are software abstractions that can migrate across the network (hence they are mobile) and represent users in various tasks (hence they are agents). Milojicic argues that some authors dislike the 'mobile' attribute and some others the 'agent' noun. Milojicic (1999) expresses that mobile agent opponents believe that most problems addressed by mobility can be equally well, yet more easily and more securely, solved by static clients that exchange messages. In contrast, those who favour mobility justify its advantage over static alternatives with benefits, such as improved locality of reference, ability to represent disconnected users, flexibility, and customization.

Kotz, Gray and Rus (2002) define a mobile agent as a running program that can move from host to host in a network. They stress that mobile agents are one form of mobile code and in its simplest form this involves dynamically installing an autonomous code on a remote host to migrate from one host to another and perform processes.

Many researchers believe that mobile agents provide great benefits on many domains. Lange and Oshima (1999) explain seven important reasons/benefits of using mobile agents for creating and designing distributed systems:

(1) They reduce the network load,

(2) They overcome network latency,

(3) They encapsulate protocols,

(4) They execute asynchronously and autonomously,

(5) They adapt dynamically,

(6) They are naturally heterogeneous and

(7) They are robust and fault-tolerant.

This literature highlights the most outstanding advantages of exploiting mobile agents. The significance of the mentioned advantages to this research is that it shows how mobile agents can solve many potential and existing problems concerning the public safety operations, i.e. reducing the network load to improve the performance and interpretability issue.

Pham and Karmouch (1998) indicate that there are some major goals for using mobile agents specially to cope with the issues around networks functionalities. They list these goals as: reduction of network traffic, asynchronous interaction, load balancing, fault resilience, data access locality and more important, agents can perform independently or cooperately with other agents to solve problems.

Macaire et al. (1999) explain that the ability of a mobile agent to transport itself from one system to another allows a mobile agent to move closer to a system that contains an object with which it wants to interact and thereby take advantage of being in the same host, or network, as that object leading to reduced network traffic, providing effective means of overcoming network latency, and perhaps most importantly, increase asynchronous communications and autonomous operations. They explain that this characteristic of mobile agents is especially interesting and effective for terminals/users that do not have a permanent connection to the network and are often disconnected for some period of time such as wireless terminals.

According to this type of literature, the most noticeable attribute of mobile agents is their ability to cope with the volatile networks and handle valuable information through the network, even when the connection has failed. This aspect of mobile agents is remarkable when the circulation of information through the network is very sensitive for applications and in situations there is heavy reliance on situational information. These network disconnections may happen more and more when the operation of the network is so dynamic and environment is extreme.

Despite the fact that there is so much literatures about the capabilities and advantages of mobile agents, some researchers show that there are considerable issues concerning mobile agents design and implementation. Pham and Karmouch (1998) list some issues in an extensive way and they mention 17 problems concerning mobile agent architecture, design and implementation, such as agent transfer mechanism, security, coordination, scalability and so forth. They categorize the root of these issues in two separate groups: those that come from the field of process migration and distributed operating systems and others that come from the field of artificial intelligence.

Reilly (2004) also investigates problems associated with mobile agents from the process migration point of view. He discusses the issues concerning a mobile agent execution language, their process persistence, communication mechanisms between mobile agents and hosts, and security issues for protecting agents and agent hosts. Reilly (2004) argues that mobile agency has failed to become a sweeping force of change and now faces competition in the form of message passing and remote procedure call technologies and it has yet to achieve widespread acceptance. Although there are significant barriers to be overcome, it does not mean that mobile agency has not its own place in research and industry since particular situations and environments will continue to use and develop mobile agents due to their great potentials.

Among all of the mentioned problems associated with mobile agents, security is one of the significant issues that requires further research effort. Milojicic (1999) refers to a number of scholars such as Dag Johansen, Dave Kotz, and Charles Petrie continuing research on security with mobile agents and spells out that there are of a lot of security issues waiting to be solved. One of the major concerns is simply the fact that mobile agents can reproduce themselves exponentially, overwhelming the entire set of computers that have mobile agent docking mechanisms (Jojansen, D. cited in Milojicic, 1999), however, most of the security problems have been solved, at least in theory (Kotz, D cited in Milojicic, 1999).  Also Reilly (2000) has a more critical view to the security issue of mobile agents. He explains that when a mobile agent leaves for a new host extreme care must be taken to prevent an unauthorized modification or analysis of the agent because they may carry confidential information and logic. Reilly (2000) also explains the potential technical problems and barriers in terms of data encryption and trusted hosts that should be taken into consideration.

Ordille (1996), Sobrado (2001) and, Ametller, Robles and Ortega-Ruiz (2004) all have developed different mechanisms to protect mobile agents and their hosts against malicious codes and unauthorized access. According to Ordille (1996) the central security concern is how to establish trust and how to limit risk for both servers (hosts) and mobile agents. Ordille (1996) suggests some mechanisms to establish an effective trust relationship between mobile agents and hosts.

Sobbado (2001) describes that in the past protection of information depended basically on the security of the hosts in which it resided. But in the age of mobile agents it is necessary to ensure protection of the code that will be executed remotely in hosts, as well as the data provided by these hosts. Sorbado (2001) proposes two different but complementary cryptographic approaches to the problem of protecting mobile agents in untrusted computing environments, since the protection strategies that are the first complete solution for protection of mobile agents in distributed computing environments.

Ametllr et al. (2004) suggest a solution for the implementation of flexible protection mechanisms for mobile agent systems in which agents protect their code and data by carrying their own protection mechanisms. They argue that their approach improves traditional solutions, where protection was managed by the platform (host). They also believe that application using mobile agents can incorporate these mechanisms to implement agent protection with minimum impact.

Vigna (1997) has proposed a protecting mechanism called ‘Action Tracing’. This mechanism is based upon the recording agent actions. As an agent executes at a host, a log is made of any actions it performs there, and the agent owner can trace the agent's actions at each host. These traces are non-deniable and allow the agent owner to check with a high degree of confidence whether there has been any threat to the agent’s state during its execution. Papaioannou (2000) says that this method is an effective method for controlling an agent’s performance. The potential drawback is that the size of the trace could be huge.

Papaioannou(2001) states that some agent protection can be gained through continual contact with the originating hosts. He provides two examples of Jumping Beans and Aglets mobile agents and argues that in a closed and controlled situation, some mechanisms such as the client/server architecture and trust based policy are useful methods to enforce security.

Kotz et al. (2002) believes that mobile agent security when execute inside a closed system is not a big concern and the security challenge is much more limited than in a general open system. They argue that most security problems fit into two categories: (1) protecting host systems and networks from malicious agents and (2) protecting agents from malicious hosts. They address the solutions to these issues especially in a closed system. Implementing a closed system could assure that the degree of security is high enough to protect the worthy and sensitive information. This is the case in a situation such as a public safety operation where a closed network is established to handle communications between personnel and units.

Despite the many concerns regarding mobile agent’s functionalities, there exists abundance of literature on interesting promises and applications of mobile agents. As Chris Rygaards and Dave Kotz (cited in Milojicic, 1999) state, mobile agents are powerful in the embedded world because these worlds are memory-constrained environments and their mobility lets users dynamically swap applications. Rynnards believes that the most powerful application of mobile agents exists in extending a mobile agent out to a remote device or node to work on the behalf of user. This can save the user a lot of effort even if the device might not have any user interface. Also, Kotz argues that mobile agents will most likely be useful in three general areas. The first is disconnected computing, such as wireless devices that frequently disconnect from the network, or use of a wireless network that might become disconnected on short notice. The second is information retrieval applications, the situation where the agent can be sent to the large data source and filter through the data locally. The third category is the dynamic deployment of software.

Research carried out by Pham and Karmouch (1998) reveals the different applications of mobile agents in telecommunication networks and network management. They describe how mobile agents can be exploited to overcome the problems concerning telecommunication networks service management and service enhancement. TINA is the mobile agent introduced by Pham and Karmouch (1998) to tackle this aim. They also made an extensive survey and review of many different mobile agent systems such as Aglet, Agent Tcl, ARA to identify different potential and practical applications for mobile agents in various areas.

According to Lange and Oshima (1999), there are no killer applications for the mobile agents because in many cases it is possible to achieve the same results by using more traditional technologies. However, for certain applications, mobile agents offer a superior solution and there are plenty of applications that benefit from using mobile agents. These include: distributed information retrieval, monitoring and notification, telecommunication network services and information dissemination just to name a few.

Many researchers believe that mobile agents could propose several attractive solutions to deal with challenges and problems in meeting bandwidth requirements and network management. Du, Li and Chang (2003) approach this topic from the network management point of view and spell out that in a volatile network environment the mobile agent and data can temporarily reside at the agent box of local hosts and they can be retraced after the connection is restored. They state that this design is suitable for an unstable network environment. Du et al. (2003) research also shows that mobile technology could considerably conserve the network bandwidth by reducing the network traffic and consequently improving the efficiency of the network management. They propose a decentralized network management framework and argue that their research results show that applicability of the mobile agents to handle the network management depends on the size of the network. If the network facilities in LANs are few, the traffic for transmitting the mobile agents will be higher than the network traffic of a centralized management architecture. But, in a large-scale network with a large number of nodes the mobile agent-based distributed network management system could be a proper option.

Moreover, Caripe et al. (1998) and Kramer et al. (1999) have carried out considerable research regarding different applications of mobile agents in telecommunication networks. Their research shows different applications and capabilities of mobile agents in terms of network management, improving wireless network performance and dealing with the volatile and dynamic situation, which is the case for most of the wireless networks. Kramer et al. (1999) describe that a wireless networks normally serves a population of frequently mobile nodes and it presents a moving target to systems designers. As a result, it is quite difficult to design a network for mobile devices, mainly because of the problem of routing packets across the wireless network characterized by a constantly changing topology. They propose a new architecture in which a collection of mobile agents cooperatively manage network services, such as mapping and routing, to cope with the perceived problem.

As Caripe et al. (1998) state, the distributed network awareness (the property of having knowledge about the current status of the underlying network resources) applications, executing in volatile network environment, should have the ability to react in response to changes in the status of the network, with the ultimate goal of minimizing the impact of these changes on the network's and service's performance. They believe that mobile agents can precisely handle a volatile network environment by moving from machine to machine while preserving their state information. They also emphasize that the mobility attribute of mobile agents allows them a more effective use of bandwidth in situations where processing should be done remotely at the data location instead of locally after downloading a large dataset.

Caripe et al. (1998) discuss the need for network-awareness in a mobile agent system and propose a mechanism for providing the necessary infrastructure to accomplish that goal. Their research focuses on active hybrid networks, a combination of reliable terrestrial links, wireless links and both fixed and volatile mobile nodes. Caripe and his colleagues state that such networks present a major challenge for any distributed application in terms of network topology, bandwidth, latency, communication links and power consumption. They argue that mobile agents have great potential and important application in this kind of environment because they can provide high availability of services on a device connected to a wireless network. Because of this, they need to be aware of relevant changes in the availability of resources and need to react accordingly in a timely fashion.

Many applications of mobile agents are of great interest in the teamwork activities and tasks such as healthcare, military and rescue situations.

Brown, Morris and Thompson (2003) apply the mobile agents for the SUO (Small Operation Unit) model and describe how mobile agents can augment the efficiency of the radio communication within the team and between the team on the field and commanders in the headquarters. Although their SUO Communicator is an email-based communication system designed for use in small operation units, it still highlights the potential capabilities of mobile agents in terms of gathering information from different sources located in a dynamic environment.

Payne et al. (2000) develop an agent-based system to support a time critical team planning task for teams. They compare the effectiveness of agent-based aiding for individual and team tasks as opposed to the traditional manual procedures of planning. Their research reveals that the agent-based system has shown to provide better decision support both for individual and team-base planning comparing to the manual system in terms of reducing the required time to make a proper decision to cope with a particular situation. However, the most considerable problem in their suggested system is the issue that agents could act like a shield between decision makers and the real situation and consequently decrease the situational awareness of decision makers and leave them uncertain as to what is being done on their behalf.

McGrath, Chacon and Whitebread (2001) research reveal that almost all of the military applications need three primary behaviors, individually or in combination. They name those behaviors as: Information Push, Information Pull and Sentinel-Style Monitoring. They exploited mobile agents to develop agent-based systems by which the three important behaviors could be established to support SUO in the battle fields and Command and Control (C2) personnel in the headquarters. Their results show that mobile agents have a considerable effect on decreasing the required time for extracting sensitive information that support decision makers need. Also they argue that mobile agents can fulfill an important requirement of SUO that is robust information dissemination across an unreliable network.

Gray (2000) provides a report on a military application of mobile agents. He argues that in the current military operations voice communication is the main way of communication. This makes it difficult for soldiers to access needed information and coordinate mission activities with other soldiers in the field or commanders in headquarters. Gray (2000) propose a communication system that exploits a wireless radio technology and mobile agents as the main manager and carrier of information that allows soldiers to query military databases, access to maps, view the position of their fellow soldiers and, so on. In their proposed system what is considerably missing and may be left for the future research are the mobile agents with the abilities to sense the network and plan their next steps. However, despite of this, their suggested system clearly shows how mobile agents could be helpful and effective to a team of soldiers in terms of providing proper information to accomplish a mission in a dynamic environment.

Hofman, McGovern and Whitbread (1998) also describe the ways that an application of mobile agents could improve the efficiency of military tactical operations in an unreliable, low bandwidth network. Also they describe notable challenges of using mobile agents across a low bandwidth communication, such as the low performance handheld computers typically connected via such links.

Agents, specially the ones that can move, have shown considerable potential and different applications in the domain of medical and casualty care. Wendelken, McGrath and Blike (2001), Greenwood, Nealon and Marshall (2003) and McGrath et al. (2003) have carried out interesting research on the medical applications of agent-based systems each of them have a different view on these applications. Hernando et al.. (2002) utilize a multiagent system to overcome the problem of finding proper data in a time critical situation and advise clinicians on diabetes treatment through a PDA.

Wendelken et al. (2001) argue that the new research and advancement of sensors diagnostic equipment could improve the combat casualty care at the individual level but they do not allow for the expedient exchange of information that is necessary to provide efficient combat casualty care. They propose an agent based medical expert system in which the sensor of a wearable computing device collects physiological data that is analyzed and distributed among the other nodes of the network. During the treatment and transportation of the injured soldier, the agent continuously moves information regarding the soldiers' health to the command personnel. Their suggested system is a good example of the application of mobile agents that could remarkably assist the C2 personnel to perceive the whole picture of the field situation and make proper decisions.

All of the reviewed applications through the above literature strongly highlight that mobile agents have remarkable potential applications to cope with the situations where environments are highly dynamic and decisions rely on the local and almost real time data and information. In this sense, the literature also shows that mobile agents can be exploited to handle this situation by probing, gathering, processing and circulating information throughout the network and help make decisions locally and centrally in effective and reliable ways.

The following section of this chapter is another literature review about other related field such as public safety and emergency first responders' task, wireless technologies and other relevant fields.

## 3.3 Review of public safety literature

According to the definitions from the US Public Safety Wireless Advisory Committee (2003) public safety service providers perform emergency first response missions to protect and preserve life, property, and natural resources and to serve the public welfare through local, State, or Federal governments as prescribed by law. Firefighters, police officers and EMS personnel fit this definition. These groups of people require suitable facilities to accomplish their tasks properly or complete them with desirable performance. Among these requirements, communications is a core requirement because it plays a key role in public safety operations and success.

A report by Thiel and Stambaugh to The United States Fire Administration report (2001) states that communications is a crucial and rapidly evolving element of public safety and fire service operations, where communication systems play a critical role for safety and effectiveness of operations. The report emphasizes that lapses in communications and radio difficulties have been contributed in numerous firefighters' deaths across the world. So, telecommunicators must be aware of the fact that interpersonal communications is the framework upon which all communication transactions are built. Furthermore, behavioural scientists believe that less than ten percent of all communication is done verbally in the public safety operations while most understanding is achieved by means such as facial expression, voice inflection, body gestures and so forth. Given this, the process is made much more difficult for the telecommunicator, who is limited to the use of radio or mobile data transmission.

The Commtech report for The US National Task Force on Interoperability (2003) states that an average of 120 firefighters are injured daily responding to or fighting fires and more than 11 civilians killed all around world everyday because of the fire accidents. This number is more overwhelming based on the report provided by the centre of fire statistics of International Technical Committee for the Prevention and Extinction of Fire (CITF) (2003). This report reveals that 28562 people have died in 2000 due to the fire events in 31 countries. This number has increased to 37214 in 2001 where the largest numbers of death were in Russia, the USA, Ukraine and China.

The Commtech report for The US National Task Force on Interoperability (2003) discusses the role of communications in the firefighters' safety and states that lack of proper communication and non-interoperability was at least partially responsible for the loss of 343 firefighters at the September 11 devastating, chaotic scene where firefighters rushed to rescue victims from the attack on the World Trade Centre.

Studies done by McGrath et al. (2003) focuses on the ways that telecommunication could be used to increase information availability on the scene to reduce the number of causalities. Their research shows that the 25% of victims (soldiers, public safety people, and civilians) killed in action or fire events die between 5 minutes and 6 hours of injury. They believe that those victims live long enough to be salvageable, but die quickly probably because of inefficiencies in the current communications and information systems. In addition to improving the outcomes of injured victims, McGrath et al. (2003) argue that a more effective flow of medical information will help to prevent injuries and of all of the casualties that medics attempt to rescue, 25% of them are already dead before the medic arrives. The process of accessing the victims puts the medic and rescue teams at risk. Ten percent of casualties in the battlefields or fire fighting operation were injured while attempting to rescue a previously injured team member. While some casualties are unavoidable, McGrath et al. (2003) believe that these specific types of injuries can be reduced and outcomes improved with a more effective analysis and distribution of medical information on the battlefields and event scenes.

These literature have four outstanding points significant to this research: First, they show how important the role of public safety services is and the ways it can serve the communities better. Secondly, they reveal that public safety providers and workers have specific requirements, among them, communications play a key role in the effectiveness and success of their services. Third, in the context of public safety, workers who are on the front line are the major commodity, and valuable resources. They need to be protected and conducted properly. Reliable communications is very important factor to achieve this goal. Finally, telecommunication is not only suffering from considerable problems but many services rely on it with implications on the civilians' and service providers' lives.

Many of the problems regarding the safety of public safety workers, go back to the nature of their operation environment. Public safety workers are the original mobile workforce. Police, emergency medical service (EMS) personnel and firefighters do most of their work away from the office, and wherever they go, timely, accurate data is essential to their work as it can often be the difference between life and death.

Wireless technology is playing an increasingly important role in tackling today's public safety issues. The adoption of wireless networking technologies means that public safety workers can effectively access data resources and communicate more efficiently with their colleagues and the dispatch. This translates into a better-served community since public safety workers are spending less time tied up in administrative processes and more time on their tasks. That's why every emergency response demands the best available information. A public safety trends for using wireless technology is to make the public safety workers in the field safer, more effective and more productive, whether in a squad car or on foot. This means getting information out where it's needed quickly, reliably and at a reasonable cost.

With wireless technology continuing to evolve, public safety agencies will embrace the ability to push even larger volumes of data out to mobile units, provide advanced functionality to public safety workers and improve their ability to protect the communities they serve. Therefore, the more the mobile data applications grow in the public safety assignments, the more need for the wireless networking becomes apparent in this field. It is important to study different wireless technologies and their capabilities to find out what they have to offer to tackle public safety issues.

Communication problems are continually cited as contributing factors in fires and emergency incidents where public safety workers are killed or injured. Thiel and Stambaugh(2001) studies on firefighters' communication issues reveals that communication problems commonly encountered by firefighters are broadly divided into two categories. First are those problems related primarily to mechanical/technical issues such as unsuitable equipment, radio malfunction, limited system capacity, or atmospheric interference. The second category of problems is somewhat broader and includes the critical human factors necessary for effective communications; for example, radio discipline and completing the communications “loop”.

The Commtech report for The US National task force on interoperability report (2003) stresses that many law enforcement officers, firefighters and emergency medical service personnel working in the same area not only cannot communicate with one another, but also in their internal communication face serious challenges especially in critical situations. Also the report spells out that the inability of the public safety commanders and officials to readily communicate with one another threatens to the public’s safety and often results in unnecessary loss of lives and property. This report emphasizes that a reliable communication and interoperability is the key to successful public safety operations and vital to public safety tasks.

Along with the requirements for reliable communication for the public safety tasks, a lot of literature has focused on the wireless technologies and its promises to deal with issues of public safety communications and information exchange. Many authors such as Careless (2002) and Griffin (2002) and different projects like the one instituted by DARPA (2001) have pinpointed some applications of mobile data and a variety of wireless technologies - especially WLANs - as a tool for improving public safety tasks performance.

Dees (2000) provides a comprehensive report on the information and communications technology for public safety. He explains the different applications of the information and communication technology (ICT) for the public safety, especially the significant applications of wireless technologies in providing the information critical to public safety tasks. As Dees (2000) describes, a wireless data system allows field units to reduce the load on their communications operators by making many inquiries and obtaining much of their operational information directly via their mobile terminals and with the appropriate software.

According to the Wireless Ready Alliance (2004), there are many advantages of using new wireless technologies over the traditional two-way communication systems in the public safety: they are more secure, more accurate, provide visual information, support and transfer different formats of information; workers can operate in the extreme environments, their performance is higher in terms of level of functionality, throughput and coverage.

This literature shows that a understanding of different wireless technologies and their promised applications is an undeniable necessity that leads to the proper adoption of technology for the public safety. The following sections are a review of the literature in which various wireless technologies will be discussed from different points of view.

## 3.4 Review of wireless technology literature

### 3.4.1 Wireless Local Area Networks

The field of wireless networks has witnessed tremendous growth in recent years and it has become one of the fastest growing segments of the telecommunications industry. Nicopolitidis et al. (2003) explain that wireless communication systems such as cellular, cordless and satellite phones as well as WLANs have found widespread use and have become an essential tool to many day to day applications. They state the biggest advantage of the wireless networks is the freedom from cables, which enables the 3A paradigm: Anywhere, Anytime, with Anyone communications.

Rogers (2004) describes from users' point of view that wireless networking is getting more popular and applicable since it connects people to each other in the more reliable and cheaper ways. Symth (2004) explains how WLANs are rapidly becoming a normal part of the communication access infrastructure and demand for WLAN products has grown dramatically over the last few years and shows no sign of slowing since it is strengthened by the growth of laptops and personal mobility products. Soon as it can be concluded, the wireless technology is a growing area in communication with interesting and promising applications that has significant impacts on the ways mobile users can communicate with each other. Among the applications, the WLAN has attracted much attention due to its interesting features and capabilities in a variety of areas and it seems to own many capabilities and functions to solve issues concerning mobile users and dynamic environments.

Wireless LANs are the one promising area that can fit the situations involving public safety communications. A lot of research has been carried out on the WLANs capabilities and issues around their deployment since WLANs have shown considerable potentials and promises in different areas. For example different WLANs protocols can cover different geographical areas and ranges (Figure 3.4).

Geier (2002), Flickenger (2003), Bing (2002) and, Alexander & Snow (2002) have conducted comprehensive research on the WLANs technologies in terms of architecture, design and also their different potential applications. Also, many pioneer companies such as Cisco, 3Com and Motorola have concentrated on the WLANs studies in order to develop and offer a variety of products, which can operate in a WLAN environment to solve perceived problems.

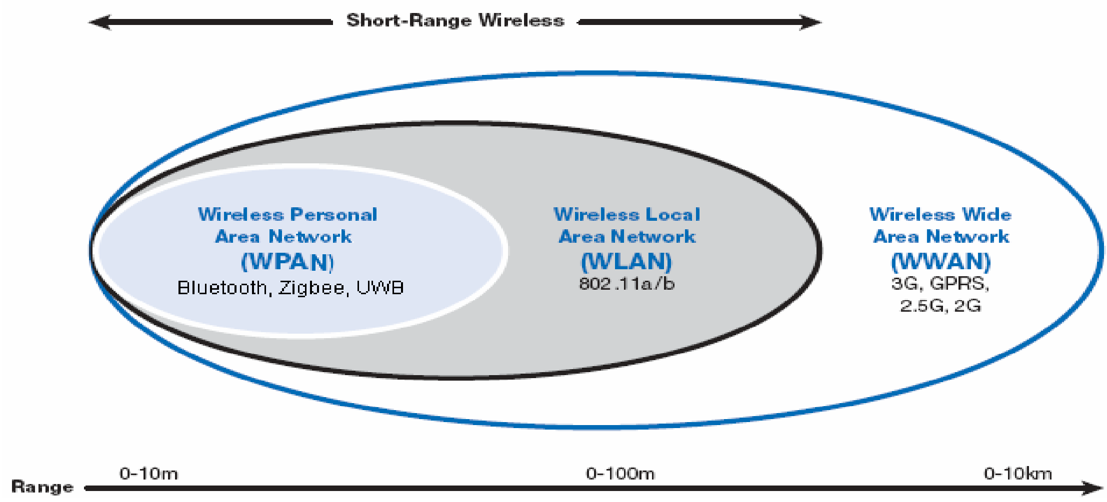


**Figure 3**.4 Classification of wireless technologies based on the coverage rang (Geier, 2000)

According to Geier (2002), wireless LANs are applicable to all industries with a need for mobile computing or when the installation of physical media is not feasible. This is the situation close to the one in which firefighters, or other public safety providers operate. WLANs are especially useful when the mobile users must process information on the spot, or front line workers need to send the updated information regarding their situation to other users.

The mobility of the users in a wireless environment has some implications on the network design and architecture. A lot of literature discusses the different arrangements and configurations in which mobility of users is taken into account in an ad-hoc fashion in order to cope with the dynamic environment.

### 3.4.2 Ad hoc Wireless Networks

According to Walker (2004), ad-hoc networks are defined as networks formed by users or devices wishing to communicate without the necessity or existence of any previous infrastructure established between potential network members. Ad-hoc communication can take place independently of any specific device, wireless transmission technology, network or protocol. Ad-hoc networks can significantly vary in size depending on applications and networks can contain two to thousands of nodes exchanging data in which they are free to enter or leave the network at any time.

Walker (2004) also shows how devices in ad-hoc networks can be diverse (laptops, PDAs, camcorders, mobile phones, sensors, etc.) and have various characteristics, like throughput, transmission power or size. More importantly, the common feature of all ad-hoc network devices is the capability to communicate using one or more wireless technologies and limited energy resources. Walker states that the initial fields for these networks were the changing environments like military applications on a battlefield. Ad-hoc networks can be established and information like position, temperature can be constantly monitored through the various types of sensors.

Smyth (2004) describes the ad hoc network as a symbiotic or parasitic network that is a network where devices make use of each other's resources in order to extend their own capacity such as data rate, power or information and the benefits of sharing these resources outweigh the negative aspects of sharing. As Smyth explains, ad hoc networks form on the fly from the communication devices themselves without needing any infrastructure or centralized control in which devices communicate directly with each other and by forming chains of transceivers they relay information through other devices in order to reach the final destination (Figure 3.5).

The above literature describes where WLANs are applicable and how they might fit the situation like public safety where tasks are often conducted in ad doc fashion. Also, they describe what kind of environments can be supported by WLANs that are similar to public safety operations.

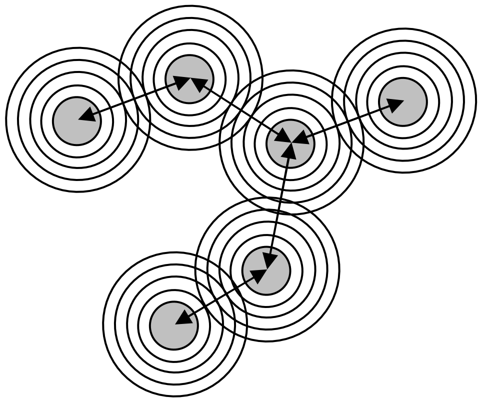

**Figure 3.5** Parasitic mobile ad hoc WLAN (Smyth, 2004)

Smyth (2004) also says that mobility is the ability to access communication services and WLAN ad hoc networks would offer users mobility within the range of base-station. This possibility has also been discussed by Engst and Fleishman (2004) as a mesh interconnections arrangement.

Nicopolitidis et al. (2003) defines the term of 'wireless ad hoc' as a network having no central administration and being comprises of mobile nodes that use wireless transmission. Each node in an ad hoc network can serve as a router by forwarding packets between stations that are out of transmission range of one another. They state the major characteristics of ad hoc wireless networks as: Distributed operation, Dynamic topology, Multihop communications, Changing link qualities and Dependency on battery life.

According to Smyth (2004), the most widely deployed application of ad hoc networks has been by the military for battlefield systems which are characterised by being insecure with no fixed infrastructure. Generally, ad hoc networks inherently are self-organising and self-healing and fit the situation where devices are moving constantly and the network is undergoing constant change that is of obvious interest of military and public safety tasks.

There are a number of technical problems regarding ad hoc networking. The most important ones are concerned with information routing through the network and securing the network in a mobile ad hoc fashion.

As a result, literature on the ad-hoc networks reveals that there is a great potential for this configuration in an environment that is changing fast and that is unpredictable. This shows that mobile ad hoc networks (MANETs) fit the situation of the public safety environment well. Implementing MANETs requires a kind of topology which could accommodate and support MANETs requirements such as flexibility and users mobility.

Bing (2002), Geier (2002) and Poor and Hodges (2002) have discussed different types of WLAN topologies. Their research shows that there are three types of WLAN topologies applied to establish a wireless connection between two or more nodes. They classify these topologies to:

1) Point-to-Point, that is sometimes referred to as a "wireless bridge" and serves as a replacement for a single communication cable and can communicate reliably as long as the two endpoints are located sufficiently close to one another to escape the effects of radio frequency (RF) interference and path loss. If a reliable connection is not initially achieved, it is sometimes possible to relocate the radios or boost the transmit power to achieve the desired reliability. This constitution shown in Figure 3.6.

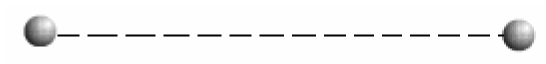

**Figure 3.6** A typical wireless bridge topology – point to point (Poor & Hodges, 2002)

2) Point-to-Multipoint such as those based on IEEE 802.11 or Bluetooth which have one base station or access point which controls communication with all of the other wireless nodes in the network. This topology is also referred to as a "hub and spoke" or "star" topology. The reliability of these networks is set by the quality of the RF link between the central access point and each endpoint. This constitution is illustrated in Figure 3.7.

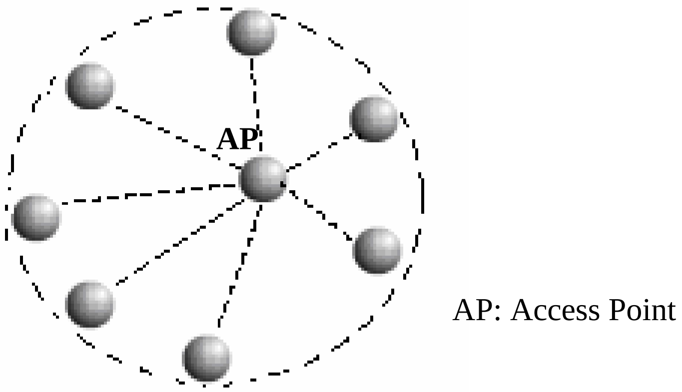


**Figure 3.7** A typical wireless Star topology – Point to Multipoint
(Poor & Hodges, 2002)

3) Mesh is a "point-to-point-to-point" or "peer-to-peer" system also called an ad hoc, multi-hop network. In this setup a node can send and receive messages and also function as a router, relaying messages for its neighbours. Through this relaying process, a packet of data will find its way to its ultimate destination, passing through intermediate nodes with reliable communication links. This constitution is shown in Figure 3.8.

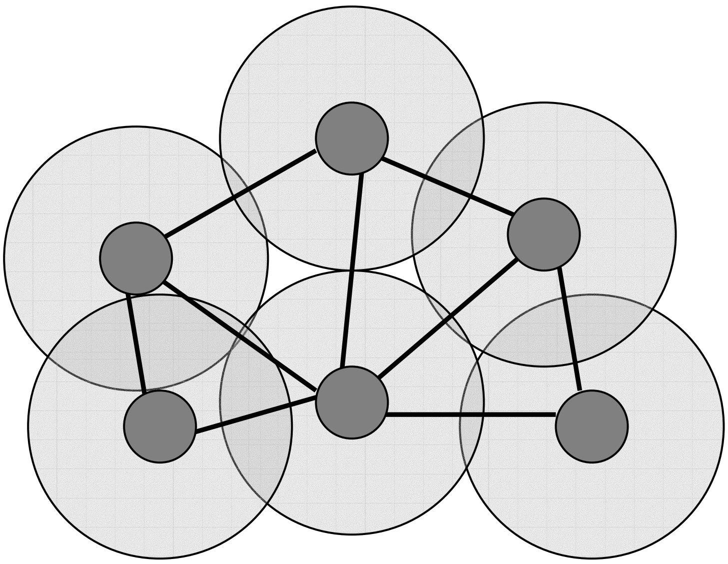

**Figure 3.8** A typical wireless mesh topology – peer to peer (Poor & Hodges, 2002)

According to Poor and Hodges (2002) mesh networking has the following characteristics and advantages:

1) Like any router-based communication networks, a mesh network offers multiple redundant communication paths throughout the network.

2) If a single node fails for any reason messages will automatically be routed through alternate paths.

3) In a mesh network, the distance between wireless nodes can be shortened which dramatically increases the link quality between nodes.

4) If a distance between two nodes reduces by a factor of two, the resulting signal is at least four times more powerful at the receiver and makes links more reliable without increasing transmitter power.

5) Greater reliability by adding new nodes as a “repeaters” in the middle of the network.

6) Self-configuring that a network discovers and adapts with the new node and automatically incorporates it into the network without the need for a system administrator.

7) A mesh network is self-healing because human intervention is not necessary for the re-routing of messages.

8) A mesh network can be deliberately "over-designed" simply by adding extra nodes so that each device has two or more paths for sending data.

9) A mesh is also scalable and can handle hundreds or thousands of nodes, since the operation of the network does not depend upon a central control point.

Poor and Hodges(2002) also stress when an environmental conditions result in poor reliability such as common in what happens in the public safety operations, it becomes difficult or even impossible to adapt a point-to-multipoint network to increase the reliability. But when the mesh networks are inherently reliable, they are adapted easily to environmental or architectural constraints. Table 3.1 shows the environmental adaptability of different topologies.

| **Topology** | **Reliability** | **Adaptability** | **Scalability** |
|---|---|---|---|
| Point-to-Point | High | Low | None (2 endpoints) |
| Point-to-Multipoint | Low | Low | Moderate (7-30 endpoints) |
| Mesh Networks | High | High | Yes (1000s of endpoints) |

**Table 3.1** Comparison of different wireless topology (Poor & Hodges, 2002)

Researchers in the Artimi company (2003) describe a mesh network as a network that:

1) Extend distance and communication speed
2) Allows effortless installation of a communication infrastructure
3) Capable of self-configuring, self diagnosis and self healing

4) Provides resiliency with no single point of failure

They add that a lightweight mesh protocol, suitable for meshes with a few tens of nodes such as ones might found in typical dynamic environment can be conveniently integrated into UWB system chip.

Whitehead (2000) states the mesh architecture as a novel alternative to the “point-to-multipoint” (PMP) architecture, which include base stations and subscriber stations. He describes a “mesh” system, as Multipoint to Multipoint (MP-MP) in which there are no base stations, only repeaters, most of which normally corresponds with a subscriber location. Connection from a service access point to a particular subscriber is via one or more successive link paths. Whitehead (2000) also spells out the considerable advantages of the mesh architecture.

1) Very high coverage levels, even at low levels of user density (more than 90% is easily achieved).

2) Excellent spectral efficiency and capacity (can be 10 to 50 times better than P-MP)

3) Low initial investment (no base stations).

4) Low interference (generated and received).

5) Complete flexibility in service delivery.

6) Built in “backhaul” links to core network access points.

7) Antenna pointing is automatic (reduced installation time).

Mesh networking technology has many potential applications for the environments without any particular infrastructure which require an agile setup of a reliable network. Broersma (2004) explains a few number of emergency responses cases where mesh networking set up play a crucial role in tackling the number of challenges such as communication interoperability, multimedia messaging and location awareness either in an indoor or outdoor area.

Among the literature some research is mainly devoted to the future applications and promises of mesh networking. Rupley (2003) describes how mesh networking technology is interesting and relevant to the military applications where the battlefield awareness application captures the promise of the mesh networking as the next wireless frontier. Rupley states that one of the most promising aspects of mesh networks is their ability to reassemble themselves to fit changing environments and many companies are now working on such mobile, flexible networks for public safety. Goodwins (2003) classifies the mesh networks to two groups of fixed mesh in which every station is fixed and mobile mesh where the stations are free to move around. According to Goodwine (2003) the three main areas needing work are security, manageability and routing.

It is worthy to mention that wireless mesh networking is an evolving concept in military, public safety and other areas. Standards are thin on the ground and standards groups are working on building mesh into the families of standards in use today. Research by Goodwins (2003), Broersma (2004), Flood and Whittle (2004) and Walker (2004) has focused mostly on the standards and protocols related to mesh networking. Among the discussed protocols and standards, Bluetooth, IEEE 802.11b (Wi-Fi), IEEE 802.15.3, IEEE 802.15.4 (Zigbee) and even 802.16 (WiMax) show and promise and are the most frequently considered technologies for use in mesh networks scenarios due to the specific features and applications that each of them can deliver.

Mesh networking is an interesting arrangement with high level of flexibility to cope with dynamic and volatile structures and it has found many types of applications. A special class of mesh ad hoc networks is that of a self-organizing network of power-sensitive sensing devices. Sensor networks coupled with the notion of ubiquitous computing have emerged as a new communication paradigm that promises to revolutionize information gathering and processing in disaster recovery (such as fire, flood and earthquake), law enforcement (crowd control, search and rescue) and tactical communications (digital battlefields), all characterized by the unpredictable changes in their environments. Integrated sensing devices permit remote monitoring in a variety of contexts.

Lewis (2004) describes the sensor networks as the key to gathering the information needed by smart environments, whether in buildings, utilities, industrial, home, shipboard, transportation systems, automation, or even anti-terrorist and guerrilla warfare where countermeasures require distributed networks of sensors and have self-organizing capabilities. In such applications, running wires or cabling is usually impractical and a wireless sensor network is required that is fast and easy to install and maintain.

Lewis (2004) also states that wireless sensor networks satisfy these requirements since desirable functions for sensor nodes include: ease of installation, selfidentification, self-diagnosis, reliability, time awareness for coordination with other nodes, some software functions and standard control protocols and network interfaces.

Also Lewis (2004) discusses the sensor as an essential element of the sensor network. He explains that the major outcome of IEEE 1451 studies is the formalized concept of a Smart Sensor where a smart sensor is a sensor that provides extra functions beyond those necessary for generating a correct representation of the sensed quantity. Included might be signal conditioning, signal processing and decision-making/alarm functions. Objectives for smart sensors include moving the intelligence closer to the point of measurement and maintaining distributed sensor systems making it cost effective to integrate creating a confluence of transducers, control, computation and communications towards a common goal, and seamlessly interfacing numerous sensors of different types. He also briefly reviews the different type of sensors such as magnetic, electric, chemical and biological sensors that could be exploited in a typical sensor network. His studies are significant to the area of public safety operations since the situations discussed by Lewis (2004) are very close to the ones in a rescue or law enforcement operation and hence the results could be applicable in this context.

De et al. (2003) and Edger and  Callaways (2003) propose a novel meshed multipath routing (M-MPR) to facilitate immediate and successful data delivery in a wireless sensor network where the network has relaxed throughput requirements often measured in a few bits per day. De and his colleagues describe that a wireless sensor network is similar to mobile ad hoc networks but it differs from them in the sense that the nodes have much reduced functionalities, such as limited transmission range and battery power and routing data are more subject to be lost. However, to recover the lost data problems concerning re-transmission of data and capabilities of sensors affect the network routing feature. They propose a routing strategy from a source to a destination based upon the mesh architecture that allows (some, if not all) nodes in the route to have more than one forwarding direction to the destination and data transmission is done via selective forwarding of packets, where the routing decision is taken dynamically, hop-by-hop, based on the conditions of downstream forwarding channels. These studies address the major concern and question of routing in a wireless sensor network and show there are solutions to deal with these issues.

Ray et al. (2003) carried out extensive research about the ways that an emergency sensor network would be used to detect a specific location robustly. They propose a new framework for providing robust location detection in emergency response systems based on the theory of identifying codes. The key idea of this approach is to allow sensor coverage areas to overlap in such a way that each resolvable position is covered by a unique set of sensors.

Ray et al. (2003) argue that communication systems play an essential role in emergency situations such as fires, building collapses or extreme weather phenomena. Existing systems often provide minimal communication infrastructure for supplying information about the nature or the extent of a disaster. As a result, first responders typically enter emergency situations with little real-time information about the site and should they become trapped, only a haphazard means of rescue becomes available to them. One promising method for providing real-time feedback from disaster sites involves the use of sensor networks. The authors also state that the recent advances in sensor technologies make it possible to install and interconnect tiny devices for networked use in the case of an emergency.

These networks could provide emergency control centres with 3D building visualization, real-time monitoring of hot spots or structure failures and tracking of victims and personnel. Central to such features is the ability to perform indoor location detection in the face of unpredictable reflections (from people, walls), occlusions (due to smoke, fire) and changing building topology (from falling walls, collapsed ceilings). Indeed, many essential tasks of an advance emergency response system require the following capabilities:

- To enable crew members to identify their own and others' location.
- To locate victims, potential hazards, or sources of the emergency.
- To identify and rescue trapped personnel.

Ray et al. (2003) studies are significant to this research due to their extensive works around the application of sensor network particularly for emergency tasks.

Patwari et al. (2003) discuss the relative location estimation in wireless sensor networks. They consider location estimation in networks in which a small proportion of devices, called reference devices, have a priori information about their coordinates. All devices, regardless of their absolute coordinate knowledge, estimate the range between themselves and their neighbouring devices. Such location estimation is called "relative location" because the range estimates collected are predominantly between pairs of devices of which neither has absolute coordinate knowledge. This research addresses one important problem and its significant requirement for the public safety operations and proposes solutions to tackle this issue. However, Patwari et al. (2003) results show that there is still need for more research to reach the accurate location estimation that can meet some specific application requirements.

As the literature shows, following the MANETs and the mesh topology, there are many potential applications of these technologies to the area of public safety in terms of dealing with volatile environments and establishing a proper structure of network that can sense the environment and support the users with the required quality of information. So it is important to understand what kind of wireless technology could be applied in such an environment and which one would be the best technology to fit the dynamic situation of public safety operations. The rest of this section is dedicated to the review of literature to investigate the potential WLANs applicable in this area.

### 3.4.3 Bluetooth

Storey et al. (2002) describes Bluetooth as the cable replacement technology by which, electronic devices can exchange information and share resources. It forms an active environment where not only physical structure but also resource availability can change as devices arrive and depart from the grouping.

According to Franklin (2003) Bluetooth has already become a global de facto standard for wireless connectivity and design-wise, the three main goals for Bluetooth were: small size, minimal power consumptionand low price. Cox, J. (2003) describe this point by stressing that Bluetooth lets nearly all devices such as cell phones, PDAs talk to one another by creating a common language between them and shape a wireless personal area network (WPAN).

Blankenbeckler (2002) explain how Bluetooth devices can interact with one or more other Bluetooth devices. As Blankenbeckler describes Bluetooth devices communicate with each other through the piconets where a piconet is any such Bluetooth network or WPAN with one master (master device is responsible to manage the composed network) and one or more slaves as illustrated in Figure 3.9.

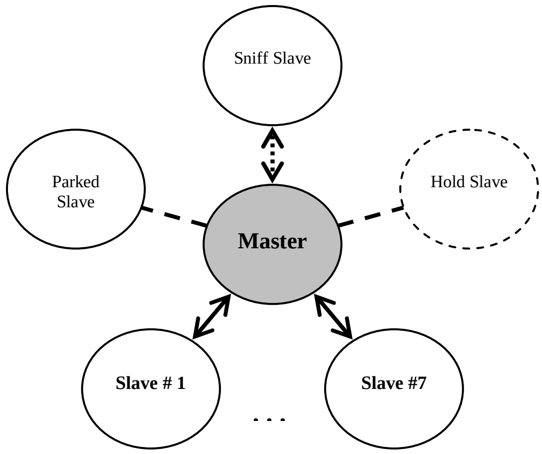


**Figure 3.9** A Bluetooth piconet with one master and up to 8 slave nodes (Blankenbeckler, 2002)

In some cases, slaves in one 'piconet' can participate in another piconet as either a master device or slave one. This scenario is referred as a 'scatternet' and discussed by Law. et al. (2001) where a scatternet is a set of piconets connected through shared devices as shown in Figure 3.10.

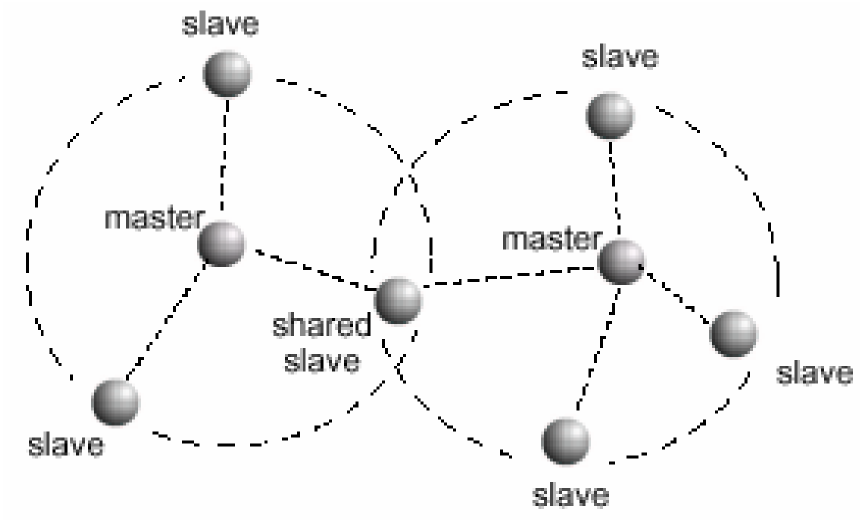


**Figure 3.10** A Bluetooth scaternet with two masters. (Law et al. 2001)

Mattisson (2000) explains a number of advantages of the Bluetooth protocol such as operation scope, flexibility in terms of design and application, cost and power consumption. However, other researches like Vainio (2000) and Golmie et al. (2004) have taken to consider the problems concerning the Bluetooth technology. Their research shows that the most of the problems and disadvantages of Bluetooth refers its security feature. In addition to the security disadvantages of Bluetooth, there are problems concerning the interference with other wireless technologies such as Wi-Fi. Another disadvantage of the Bluetooth is that it has a coverage range limitation of 10m since it has originally been designed as a way to replace cables.

Arensman, (2003) carried out some studies to compare Bluetooth with some other promising protocols such as Zigbee and Wi-Fi from different aspects and Arensman's findings are summarized in table 3.2.

| Wireless Standards | Bluetooth | ZigBee | Wi-Fi |
|---|---|---|---|
| **Frequency:** | 2.4 GHz | 2.4 GHz (global)<br>915 MHz (Americas)<br>868 MHz (Europe) | 2.4 GHz (802.11b)<br>5 GHz (802.11a) |
| **Range:** | 10 meters | 30 meters | 100 meters (802.11b)<br>50 meters (802.11a) |
| **Transmission rate (Kbps):** | 1,000 | 250 | 11,000 (802.11b)<br>54,000 (802.11a) |
| **No. of devices supported:** | 8 (each piconet) | 255 | 50 (802.11b)<br>250 (802.11a) |

**Table 3.2** Comparison table of Bluetooth and other wireless standards (Arensman, 2003)

Looking at the specifications and capabilities of the Bluetooth standard as a wireless protocol, it can be seen that although Bluetooth is a dominant wireless standard for the low rang cable replacement there are still considerable questions about its capabilities in terms of propagation and penetrations in indoor and outdoor spaces. Also Bluetooth seems to have some restrictions in supporting too many nodes on the move and pinpoint the mesh networking topology due to that fact that it's best suited to the point-to-multipoint topology.

### 3.4.4 Zigbee

Technically, Zigbee is a protocol standard that defines network, security and application framework protocol software. Zigbee is designed to work on top of the IEEE 802.15.4 PHY/MAC layer standard. According to the documentation widely available on the Zigbee website, www.zigbee.org, the benefits that the Zigbee standard provides are:

- Reliable and self-healing
- Supports a large number of nodes
- Easy to deploy
- Low cost
- Long battery life
- Secure
- Global deployment

Additionally, the website claims that the standard has several benefits over proprietary solutions:

- Product interoperability
- Vendor independence
- Increased product innovation

As Galeev (2004) and Kinney (2003) describe, Zigbee, based on IEEE 802.15.4, is a low-power, low-data-rate wireless networking standard designed specifically for remote monitoring and control applications. IEEE 802.15.4 ratified in May 2003 and is a simple but powerful packet data protocol that provides high reliability through acknowledgement, error checking, prioritized communications, direct sequence spread spectrum, the ability to change frequencies to avoid interference and user-selectable security levels. IEEE 802.15.4 specifies the physical (PHY) and media access control (MAC) layers and defines three license-free frequency bands including 2.4 GHz, 915 MHz and 868 MHz, offering users an alternative regional frequency if the 2.4 GHz band is not optimal for a particular application. Per node transmission ranges from 30m to100m are possible and the transmission distance can be extended through the use of power amplifiers and multi-hop mesh networking.

Exploring the Ziggbe standard reveals that Zigbee supports three networking topologies: star, mesh and cluster tree. As Galeev (2004) states star networks are common and provide for very long battery life operation. Mesh networks enable high levels of reliability and scalability by providing more than one path through the network. Cluster-tree networks utilize a hybrid star/mesh topology that combines the benefits of both for high levels of reliability and support for battery-powered nodes. These three constitutions are illustrated in figure 3.11.

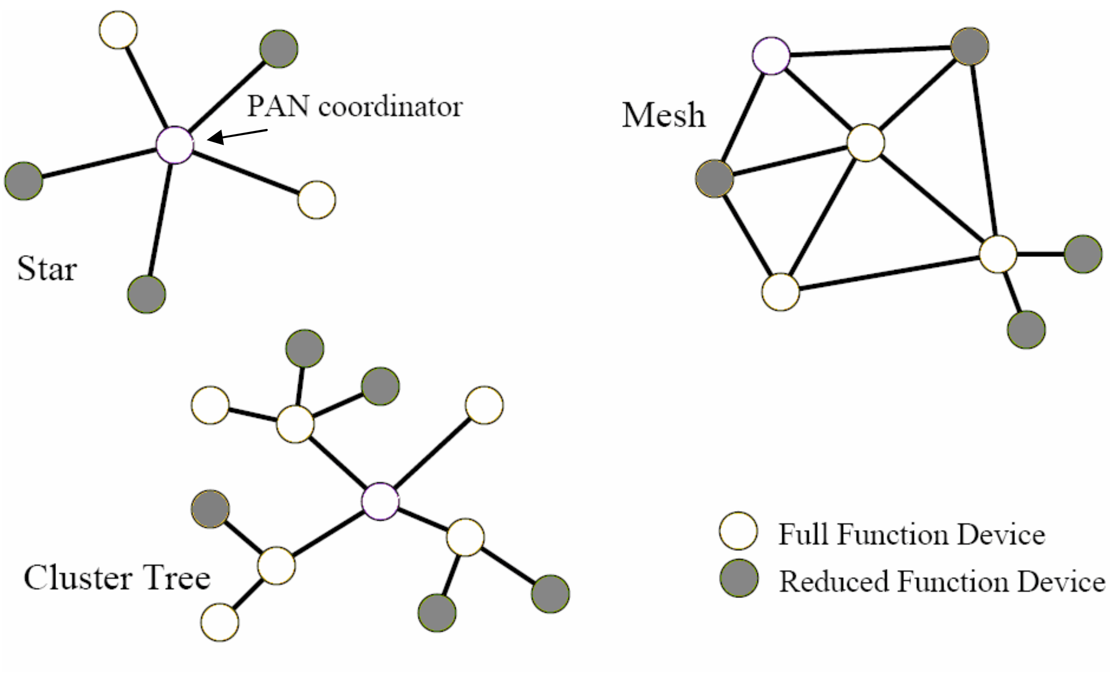


**Figure 3.11** Different types of topologies supported by Zigbee (Craig, 2004)

Craig (2004) has carried out extensive studies about the Zigbee standard devices. According to Craig (2004), to provide for low cost implementation options, the

Zigbee Physical Device type distinguishes the type of hardware based on the IEEE 802.15.4 definition of reduced function device (RFD) and full function device (FFD) where an IEEE 802.15.4 network requires at least one FFD to act as a network coordinator. The specifications of these types of devices are summarized in the following table (Table 3.3):

| **Reduced Function Device** | **Full Function Device** |
|---|---|
| Limited to star topology | Can function in any topology |
| Cannot become a network coordinator | Capable of being a Network coordinator |
| Talks only to network coordinator (FFD) | Capable of being a coordinator |
| Simple implementation – min RAM and ROM. | Can talk to any other device (FFD/RFD) |
| Generally battered powered | Generally line powered |

**Table 3.3** Zigbee physical device types

Craig (2004) explains that an RFD can be implemented with minimum RAM and ROM resources and it is designed to be a simple send and/or receive node in a larger network. Also RFDs can only talk to an FFD, a device with sufficient system resources for network routing. On the other hand the FFD can serve as a network coordinator, a link coordinator or as just another communications device. Any FFD can talk to other FFD and RFDs. FFDs discover other FFDs and RFDs to establish communications and are typically line powered.

Craig (2004) explains that Zigbee Logical Device type distinguishes the Physical Device types (RFD or FFD) deployed in a specific Zigbee network. The Logical

Device types are Zigbee Coordinators, Zigbee Routers and Zigbee End Devices. The Zigbee coordinator initializes a network, manages network nodes and stores network node information.

Zigbee’s self-forming and self-healing mesh network architecture permits data and control messages to be passed from one node to other node via multiple paths. This feature extends the range of the network and improves data reliability. Montgomery (2004) explains this as the peer-to-peer capability that may be used to build large, geographically dispersed networks where smaller networks are linked together to form a ‘cluster tree’ network. Zigbee provides a security toolbox to ensure reliable and secure networks. Access control lists, packet freshness timers and 128-bit encryption protect data transmission and Zigbee wireless networks.

Despite the fact that Zigbee shows many potential applications and promises in the area of MANETs, there are many concerns about the Zigbees’s functionalities as well. Frank (2004) argues that although Zigbee provides very low power connectivity– much less than Wi-Fi and less than Bluetooth, this is also a drawback for transferring data to a higher range.

According to  Smith (2003) ZigBee was relatively slow. It transmits its data at about 250 kilobits per second (compared with Wi-Fi's 11-54 megabits and Bluetooth's 800 kbps) over fairly short distances.

In summary, the literature about the Zigbee standard could support a mesh topology and moving nodes. However, the application of Zigbee in public safety environments can be limited due to the kinds of devices it can support and types of communication it can provide. In other word, Zigbee is not basically designed to operate in extreme environments such as those of rescue or law enforcement tasks.

### 3.4.5 IEEE 802.11

A wireless local area network (WLAN) uses radio frequency (RF) technology to transmit and receive data over the air. The Institute of Electrical and Electronics Engineers (IEEE) has established the IEEE 802.11 standard, which is the predominant standard for wireless LANs. Any LAN application, network operating system, or protocol including TCP/IP, will run on 802.11-compliant WLANs as they would over Ethernet. WLAN transmits on unlicensed spectrum as agreed upon by the major regulatory agencies of countries around the world although there is some variation by country.

According to Zyren and Al Petrick (2004), and Nicopolitidis et al. (2003) there are two different ways to configure a network in IEEE 802.11 architecture: ad-hoc and infrastructure. In the ad-hoc network, computers are brought together to form a network "on the fly" using a peer-to-peer setup. There is no structure to the network, there are no fixed points, and usually every node is able to communicate with every other node. Chen (1994) also spells out that although it seems that order would be difficult to maintain in this type of network, algorithms such as the spokesman election algorithm (SEA) have been designed to "elect" one machine as the base station (master) of the network with the others being slaves. Another algorithm in an ad-hoc network architectures uses a broadcast and flooding method to all other nodes to establish who's who.

The WLAN standards began with the standard, developed in 1997 by the IEEE. Geier (2002) explains that 802.11 base standards allowed data transmission of up to 2 Mbps and it can support multiple data rates to accommodate the loss of signal strength while maintaining high quality in data packet reassembly. Over time, this standard has been enhanced. These extensions are recognized by the addition of a letter to the original 802.11 standard, such as 802.11a, 802.11b and 802.11g are the most popular standards among others. These are listed in table 3.4.

| 802.11 | The original WLAN Standard. Supports 1 Mbps to 2 Mbps. |
|---|---|
| **802.11a** | High speed WLAN standard for 5 Ghz band. Supports 54 Mbps. |
| **I802.11b** | WLAN standard for 2.4 Ghz band. Supports 11 Mbps. |
| **802.11e** | Address quality of service requirements for all IEEE WLAN radio interfaces. |
| **802.11f** | Defines inter-access point communications to facilitate multiple vendor-distributed WLAN networks. |
| **802.11g** | Establishes an additional modulation technique for 2.4 Ghz band. Intended to provide speeds up to 54 Mbps. |
| **802.11h** | Defines the spectrum management of the 5 Ghz band for use in Europe and in Asia Pacific. |
| **802.11i** | Address the current security weaknesses for both authentication and encryption protocols. The standard encompasses 802.1X, TKIPand AES protocols. |

**Table 3.4** IEEE 802.11 different standards and their specifications (Geier, 2002)

Bing (2003) and Flickenger (2003) have carried out comprehensive studies regarding different features of IEEE 802.11a, b and g. Their studies show that each of these standards qualifies for different types of applications. For example, the frequency at which 802.11b and 802.11g transmit allows it to penetrate solid materials allowing, in most indoor environments, a maximum range of 300 feet. 802.11a experiences a steeper decline in throughput as distance increases from the access point and has a maximum range of about 150 feet in most indoor environments. The range and transmission speed is affected by the environment in which the WLAN is deployed.

Also King (2001) explains that the 802.11a specification operates at radio frequencies between 5.15 and 5.875 GHz and the 802.11b and 802.11g specification operates at radio frequencies in the 2.4 to 2.497 GHz range, so the 802.11a has a wider frequency band allowing more channels and more overall throughput. As the result, the wider frequency band allows 802.11a to support up to eight non-overlapping channels and 802.11b/g to support up to three non-overlapping channels although the frequency ranges and channels may vary by country.

Smyth (2004) explains that each channel will carry a maximum throughput for its standard. Therefore, the 802.11b and 802.11g standards have a maximum of three non-overlapping channels carrying 11 Mbps throughput each (33 Mbps total) and 54 Mbps (162 Mbps total) throughput. The 802.11a standard has a maximum of eight non-overlapping channels carrying 54 Mbps throughput each, or 432 Mbps total throughput. He concludes that the advantage of 802.11b is that it's the most widely deployed wireless LAN technology and provides good wall penetration and indoor range and the advantage of 802.11a is it provides increased network capacity and lower interference with other wireless devices than 802.11b.

Studies in the 3COM (2003) company shows that there are specific differences among the three major IEEE 802.11 technologies as the following table (Table 3.5) shows:

| Standard | Radio Band | Modulation | Max. Link Coverage | Max. Data Rate | Max. # Non-overlapping channels | Other Issues |
|---|---|---|---|---|---|---|
| **802.11b** | 2.4 GHz | DSSS | 100m/328ft | 11 Mbps | 3 | - 802.11b networks have the largest installed base. |
| **802.11a** | 5 GHz | OFDM | 50m/164ft | 54 Mbps | 12 | - Needs 802.11 extensions to be used in some regions |
| **802.11g** | 2.4 GHz | OFDM | 100m/328ft | 54 Mbps | 3 | - Backward-compatible with 802.11b<br>- Fully ratified |

**Table 3.5** Comparison of 802.11a, 802.11b and 802.11g (3COM, 2003)

Also Nelson (2002), Marci (2003) and Struhsaker (2003) have carried out research around the IEEE 802.11 issues, specially the ones concerning the network security. Their studies show that security is the most considerable concern for the IEEE 802.11 a, b and g development. These are described as the vulnerabilities of IEEE 802.11 series and many methods and algorithms are proposed to cope with these pitfalls.

Most of the research like the ones done by Alexander and Snow (2002), McFarland & Wong (2003) and Poor and Hodges (2002) shows that the IEEE 802.11a, b and g are suitable for the point-to-multipoint configuration although there are a number of articles that have a look at these technologies from a mesh topology perspective. But significantly the literature doesn't seem confident on the feasibility of these technologies for the mesh configuration. Instead it is mostly positive about the point-to-multipoint make up.

Research shows that IEEE 802.11x series have interesting features applicable in establishing a wireless connection between nodes on the move. However, considering the public safety environment, IEEE 802.11x series seem have the capability to support the mesh topology but it is not as effective as UWB since it is mainly designed to work as a wireless protocol in a point to multi point wireless connection. Also it can operate in the frequency spectrum where there is a great chance of interferences with other wireless devices and this is undesirable feature for the public safety tasks operations.

### 3.4.6 Ultra Wide Band (UWB)

Ultra Wideband is an innovative wireless technology that can transmit digital data over a wide frequency spectrum with very low power and at very high data rates. As well as having the ability to transfer high-speed data using low power, Ultra Wideband can carry signals through many obstacles that usually reflect signals at more limited bandwidths and at higher power. In addition to the high data rate capability of Ultra Wideband its low transmit power also means it transmits negligible interference to existing systems. The low power properties of Ultra Wideband communications can allow systems to operate across a range of frequency bands unlicensed. The power is so low in fact, that it is below the levels associated with the emission limits for unintentional transmitters such as televisions and washing machines.

Researchers at Motorola Inc. (2003) describe the Ultra-wideband as a wireless technology that transmits an extremely low power signal over a wide swath of radio spectrum, achieving data rates as high as 114 Mbps data transfer rate supporting applications such as streaming video, streaming audio and high-rate data transfer at very low levels of power consumption.

They state that unlike conventional radio systems that operate within a relatively narrow bandwidth, like Bluetooth, IEEE 802.11a/b/g, ultra-wideband operates across a wide range of frequency spectrums by transmitting a series of very narrow and low power pulses (Figure 3.12). The combination of broader spectrum, lower power and pulsed data means that ultra-wideband causes less interference than conventional narrowband radio solutions and delivers wire-like performance in an indoor wireless environment. This research has an important point that describes what are the major differences between UWB and other popular wireless standards specially from bandwidth and frequency spectrum.

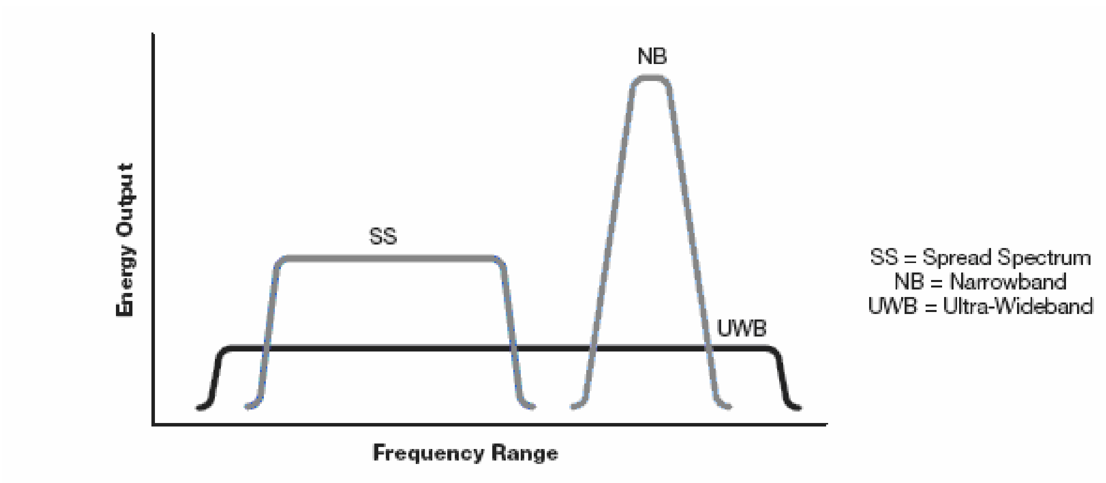


**Figure 3.12** Comparison of narrowband spread spectrum and Ultra-wideband signal (Hulter & Streeton 2003)

Kolic (2004) explains the different methods of the UWB communication and classifies them into traditional and modern methods. As he explains, a traditional UWB transmitter works by sending billions of pulses across a very wide spectrum of frequency several GHz in bandwidth. The corresponding receiver then translates the pulses into data by listening for a familiar pulse sequence sent by the transmitter. Modern UWB systems use other modulation techniques, such as Orthogonal

Frequency Division Multiplexing (OFDM), to occupy these extremely wide bandwidths. In addition, the use of multiple bands in combination with OFDM modulation can provide significant advantages over traditional UWB systems. The Multi-Band OFDM approach allows for good coexistence with narrowband systems such as 802.11a, adaptation to different regulatory environments, future scalability and backward compatibility. This design allows the technology to comply with local regulations by dynamically turning off sub-bands and individual OFDM tones to comply with local rules of operation on allocated spectrum.

Kolic (2004) also states how the dynamic ability of the radio to operate in certain areas of the spectrum is important because it can adapt to regulatory constraints imposed by governments around the world.

Zasowski et al. (2003) have carried out interesting research on the Wireless Body Area Networks (WBANs) and applications of UWB in this area. WBANs are networks whose nodes are usually placed close to the body on or in everyday clothing. A WBAN topology comprises many transmit only sensor nodes, that have to be very simple, low cost and extremely energy efficient, some transceiver nodes, that afford a somewhat higher complexity to sense and act and few high capability nodes, e.g. master nodes with high computational capabilities and support for higher data rates.

According to Zasowski1 et al. (2003), compared to other wireless networks a WBAN has some distinct features and requirements. Due to the close proximity of the network to the body, electromagnetic pollution should be extremely low. Thus, a non-invasive WBAN requires a low transmit power. Therefore a multihop approach is promising where a sensor does not transmit its data directly to a master node but the data is forwarded by several nodes. Furthermore WBANs have a special network topology since it is given by the shape of the human body. In contrast to indoor channels, the permanent presence of the body could lead to deterministic channel characteristics which could be exploited to simplify the receiver design. They conclude that a possible technology for non-invasive WBAN communication is Ultra Wideband. This research focuses on the many interesting aspects of the UWB such as energy efficiency and sensor adaptation which are very interesting to the public safety operations.

Fontana et al. (2002) also describe the applications of UWB in government communications areas. As they state, both tactical and strategic applications are of importance, with low probability of detection (LPD) a primary requirement in most government applications. They provide an overview of three developed UWB systems which were designed to meet tactical, strategic and mixed-mode requirements for LPD multi-user communications. This research strongly shows how unique characteristics of the UWB could make it a more secure technology and free from the concerns of detection and intervention that are desirable to many tactical and strategic applications.

Amet et al. (2003) also discuss the development of an aircraft wireless intercommunications system (AWICS) which utilizes ultra wideband technology to address mission requirements for the multi-crew, military aircraft. In their proposed system, UWB offers unique advantages in this application due to multipath mitigation, low probability of detection, low probability of interference to onboard legacy systems and high throughput in a multi-user environment. Amst et al. (2003) research results reveal that UWB has been shown to have unique performance advantages for wireless transmission within severe multipath environments such as those encountered onboard aircraft. These advantages stem largely from the use of large bandwidth waveforms which, in the time domain, can be resolved from a multitude of multipath returns. In addition, the correspondingly low average power densities of a UWB waveform have advantages for both low probability of detection and low probability of interference with onboard legacy systems.

Steve Rowe (2003) has focused on the medical applications of the UWB. He states that as well as the ability to transfer high-speed data in a low power fashion, UWB can also provide a reliable location information and high resolution imaging and works well in a cluttered environment.

Although UWB seems to have very interesting applications in many areas there are still considerable problems concerning its effective application that need to be addressed. Hamblen (2004) describes that UWB faces serious regulatory hurdles and it is hard for it to move forward. As Hamblen(2004) states, UWB radios and regulators worry that UWB will interfere with a range of other wireless devices that operate in the same spectrum, including cell phones.

Kolic from the Intel Inc. (2004) believe that for UWB technology to become a widely adopted radio solution, a few key areas need to be resolved:

- Global spectrum allocation

- Performance (including over-the-air data rate performance, power consumption, co- existence with other wireless devices, immunity to interference and link robustness)
- Interoperability
- Ease of product integration and certification
- Fulfilment and support

Also Research carried on the UWB out by Miller (2003) shows that there are different advantages, disadvantages and applications concerning UWB waveform properties. His results are shown in brief as the following table (Table 3.6):

| UWB Property | Advantages | Disadvantages | Applications |
|---|---|---|---|
| Very wide fractional and absolute RF bandwidth | • High rate communications<br>• Potential for processing gain<br>• Low frequencies penetrate walls, ground2,4 | • Potential interference to existing systems<br>• Potential interference from existing systems | • High-rate WPAN<br>• Low-power, stealthy communications<br>• Indoor localization<br>• Multiple access |
| Very short pulses | • Direct resolvability of discrete multipath components<br>• Diversity gain9 | • Large number of multipaths<br>• Long synchronization times | Low-power combined communications and localization |
| Persistence of multipath reflections | • Low fade margins<br>• Low power | Scatter in angle of arrival | communications indoors and on ships |
| Carrierless transmission | • Hardware simplicity<br>• Small hardware10 | Inapplicability of super-resolution beam-forming | Smart sensor networks |

**Table 3.6** UWB specifications and applications (Miller, 2003)

Poor and Hodges (2002) extensively describes how UWB could be fit a mesh configuration and could be used to setup a high performance mesh network. They explain that UWB technology can transmits data at a rate exceeding 1 billion pulses per second and spreads the transmissions across the widest possible frequency band. Based on these arguments they list the interesting features of UWB that makes it more appealing to arrange a mesh network configuration.

UWB devices can perform a number of useful telecommunication functions that make them very appealing for both the commercial and government applications. These systems have very wide information bandwidths, are capable of accurately locating nearby objects and can use processing technology with UWB pulses to "see through objects" and communicate using multiple propagation paths.

Sachs et al. (2002) discuss the Ultra wideband radars applications such as surface penetrating radar, surveillance and emergency radar, medical instrumentation, non-destructive testing in civil engineering and the food industry, industrial sensors and microwave imaging and many others. They also explain how an UWB radar is able to detect hidden objects and a high bandwidth not only results in good spatial resolution but also in improved capabilities for object recognition. They also have a look at the sensors which work with UWB and state that an UWB-sensor is built from three main parts of applicators, the measurement electronics and the processing software. This research has a military application approach but it could still be applicable to the area of public safety since there are many common features in terms of requirements and environment for both of these areas.

According to Chapman (2002) the current technologies such as IEEE 802.11a offers data rate up to 54Mbit/sec, whilst emerging UWB technologies promise to push the capacity boundary beyond 100Mbits/sec. He made a comparison between different wireless technologies and illustrates this idea through the following figure (Figure 3.13):

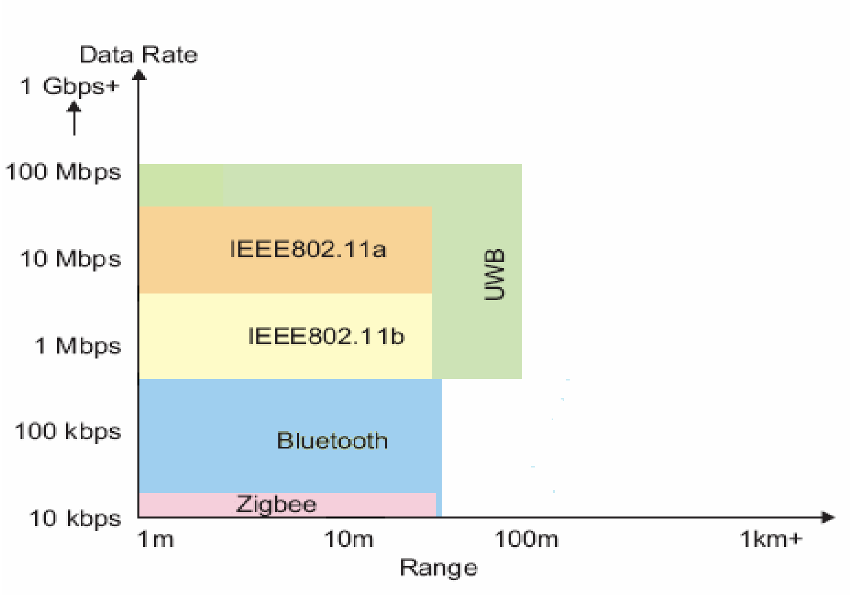


**Figure 3.13** Different wireless technologies range and data rate (Chapman, 2002)

Bing (2002) discusses the different methods that UWB spectra can be generated and discusses the specifications and potential application of each of the UWB generation methods. These studies also are important to this research since adoption of proper technology which could satisfy the users', providers' and civilians' requirements is a remarkable issue.

## 3.5 Review of Wearable Computing literature

One other important area related to the networking technology is sensors. These sensors might be embedded in the users' clothes or attached to a particular device in order to sense the environment of operation. These sensors not only can sense the environment but also might able to perform degrees if processes on the spot. These kinds of matter are mainly discussed through the area of wearable computers.

Wearable computers are body-mounted, interactive computing devices designed for applications where operators are required to be mobile, keep their hands free, view data in bright sunlight or darkness and/or keep a largely undisturbed view of the environment while viewing computer or video data. So, a wearable computer is a computer that can be worn, like tools, clothing and glasses and interact with the user based on the context of the situation. With head-up displays, unobtrusive input devices, personal wireless local-area networks (LANs) and other context-sensing and communication tools, the wearable computer can act as an intelligent assistant wherever the user is.

Mann (1998) describes a wearable computer as a computer that is subsumed into the personal space of the user, controlled by the user and has both operational and interactional constancy, i.e. is always on and always accessible. Mann (1998) states that a computing device most notably is a device that is always with the user and into which the user can always enter commands and execute a set of such entered commands and in which, the user can do so while walking around or doing other activities.

Mann also formally defines a wearable computing device in terms of its three basic modes of operation and its six fundamental attributes in interaction between human and computer:

- Constancy: The computer runs continuously and is ``always ready'' to interact and runs continuously to provide a constant user interface.
- Augmentation: Wearable computing is based on the notion that computing is NOT the primary task. The assumption of wearable computing is that the user will be doing something else at the same time as doing the computing. Thus the computer should serve to augment the intellect, or augment the senses.
- Mediation: The wearable computer can encapsulate users. It doesn't necessarily need to completely enclose users but the concept allows for a greater degree of encapsulation than traditional portable computers. There are two aspects to this encapsulation:
    - Solitude: It can function as an information filter
    - Privacy: Mediation allows users to block or modify information leaving the encapsulated space.

Mann (1998) finally concludes that the wearable computing is a framework for enabling various degrees of each of these three fundamental modes of operation.

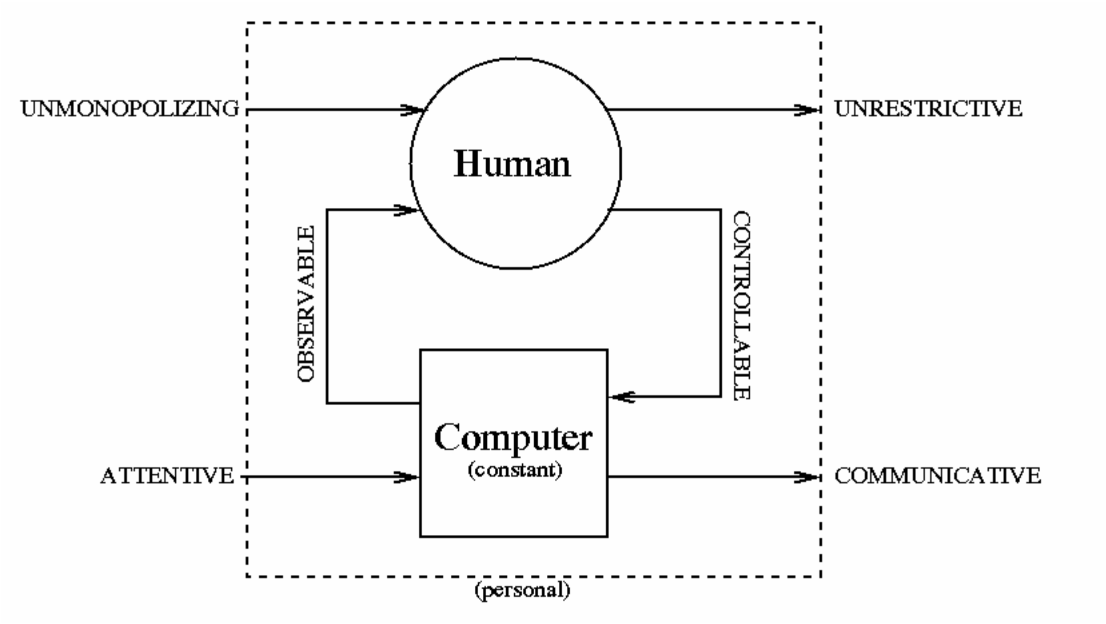


**Figure 3.14** Attributes of wearable computing devices in interaction with humans Mann (1998)

He also states that there are six informational flow paths associated with this human-machine synergy. These signal flow paths are, in fact, attributes of wearable computing and are described, in what follows, from the human's point of view (Figure 3.14):

1) Unmonopolizing
2) Unrestrictive
3) Observable
4) Controllable
5) Attentive
6) Communicative

Mann's studies are significant to this research since it provides a framework and vision for the application of wearable computing devices. It assist to identify the interesting features of wearable computing devices and apply them in the situations where there are needs to hand over users' task to the smart devices for any reason.

Santoyo (2003) approaches this topic from applications point of view. She states that wearable computers are demonstrating quantifiable benefits for workers such as field-service technicians, police officers and the armed forces and today, wearable computers can be found on field-service people who need to access data wirelessly from a central computers or databases. As Santoyo (2003) explains the rescue personnel have a usage pattern similar to field-service technicians, with the need to access information quickly from a database. Additionally, they are often required to provide reconnaissance information to a command post.

By using a wearable computer, the officer can immediately enter and retrieve information without leaving the scene. She also states that wearers need to be able to "see" their environment, store information, communicate record and stream video and large amounts of data, operate sensor devices and facilitate unprecedented command and control. The importance of Santoyo's research is that it shows how wearable computing devices could be applicable to any field-services where the flow of information significantly contributes to the success of process. This application is considerable especially for the emergency and rescue tasks where information would have great impact on lives.

Knight (2002) discusses the research at Boeing and the MIT's Media Laboratory which developed a computer system that could be installed into a conventional space suit. He explains how wearable computing devices could be employed to cope with critical situations like the ones that might happen in spacecrafts. As Knight (2002) states the wearable computing devices equipped with a camera have important application to unforeseen engineering problems like the situation where an astronaut is unable to solve a problem video could be uploaded from the ground to the station and then shown to the astronaut. A similar situation might also happen in the public safety operations. So, Knight (2002) studies give a better understanding of wearable computing applications in the situations where a solution to a particular problem needs remote consultations with experts through information exchange.

Theil (2001) has a more critical look at the area of wearable computing devices. He spells out that there are many challenges concerning the applicability of wearable computing including:

- How these devices can fit the considered infrastructure
- How to minimize their weight and bulkiness
- How and where to locate the display
- What kind of data entry device to provide.

Child (2003) research is focusing on the networking of wearable computers and related technologies. He discusses a scenario where 5000 soldiers and vehicles report back to central command in a hub network environment and believes that the traditional networking could not handle this scenario. He proposes an ad-hoc, self-configuring multi-path network which make more sense and applies the Wi-Fi wireless technology to arrange the ad-hoc network, a solution that’s probably applicable to military applications. He proposes a personal server concept: a small, mobile device that is designed to hold all of its user’s personal information where the device has no physical input/output capabilities. Rather, it links wirelessly to displays and other I/O devices in the local environment, enabling users to access the contents of the device wherever they travel. Essentially, it enables any computer, with a small amount of additional software installed, to perform as if it were the user’s own computer.

Evan, Chandler and Nobel (2002) propose a threat response system which offers a compelling application for wearable computers. In threat response and prevention applications, immediate access to information enhances the responders’ effectiveness and reduces the risk to their safety. Typically, however, the primary task requires the full attention, unobstructed vision and free use of both hands of each team member and this would be hindered by using even small handheld computers. Thus ergonomic wearable displays are an enabling technology for these critical wearable computers applications. According to Evan et al. (2002) military and civilian threat response provides a compelling application for wearable computers. On the one hand the individuals in emergency situations must have completely unrestricted mobility. On the other hand they should be armed with as much information and data as they can get effectively utilize. The author described the Digital MP Program, which provides military police with face recognition, navigation and mapping, information gathering, translation and communication functions either on the base or on missions anywhere in the world. Similar conditions exist in civilian applications such as airport security or firefighters tasks.

# Chapter 4

# Analysis of results

## 4.1 Introduction

The application of wireless technology and mobile agents to the public safety domain and rescue operations was evaluated by examining a comprehensive recent case, a portion of the September 11 of 2001 World Trading Centre collapse. The main reason to adopt this approach is that case studies have provided an established, valuable method of study. Case studies are exploited in many disciplines as Yin (2003) stated that the case study is a “frequent mode of thesis and dissertation research in psychology, sociology, political science, anthropology, history and economics and engineering”. It is significant to understand that the frequent use of case studies is due to the fact that they allow close in-depth analysis and understanding of specific cases, aid in understanding unique realms of inquiry, and provide insight into cases that could not be duplicated experimentally. As it is mentioned earlier in this thesis, relaying on a single case could be useful if the case is comprehensive and there is enough evidence and information about it.

A case study, as applied to this thesis, involves the investigation into the series of social and technical phenomena. In this study, the September 11, 2001 World Trading Centre (WTC) towers collapse. The case study applied in this research is so called a "secondary case study". This means that thesis uses the information and results of the previous case studies in the context of this research in order to investigate the research question. This approach provides us with the advantages of high reliability of the documents and available information about the case. Also it is along with the intention of this research to look at the previous case from different perspective which can provides us with new insight and results appealing to this research.

## 4.2 Review of the September 11, 2001 WTC Collapse

### 4.2.1 Background

Background knowledge of the WTC collapse studied in this thesis can provide insight into the communication processes, complex interactions, and the accident sequences itself. This is a general overview from the first aircraft's hit inception to the time of the second tower collapse. A more complete account can be found in the published literature and reports cited in this thesis.

This case study uses the materials and reports provided mainly by US National Commission on the Terrorists Attack upon the United States (2004) and "The Fall of the World Trade Centre" documentary made by BBC network on 2003. The case study will briefly investigate the primary reasons that enforced each of the towers fall down after they had been hit by aircrafts. This view provides a valuable insight to the conditions that each of the towers went through after it had been hit. Respectively, it would help the readers to understand better how radical the environment was, from the time zero (first hit) until the last moment the second tower collapsed. Furthermore it can provide a better insight to the crucial role of communications systems which could lead the decision makers to make appropriate decisions in a timely fashion based upon different kinds of data they receive from different of sources. These points are the primary themes of this case study in order to show how the later proposed communication system and suggested framework could endorse the important role of information sharing among different parties, particularly, in an extreme environment.

### 4.2.2 First hit on the World Trade Centre

In the September 11, 2001 the two most famous buildings in the world were ruined. Even today, may people believe that the remained rubbles on ground-zero has the capacity to shock people because whatever happened there on the September the 11 still seems beyond the comprehension. A lot of research has been carried out since that time to clarify how two of the world's tallest skyscrapers could have been destroyed so quickly. Disaster on this scale begs two crucial questions. Was it possible to save more lives before and during the collapse of buildings? Why so many people, including too many firefighters, died in the event?

According to Bock (2002), many after-action reports reveal that many of the firefighters in the second World Trade Centre tower, before it started to collapse simply didn't know that their commanders had ordered them out. They didn't know that a police helicopter hovering outside the Tower had indicated almost a half an hour before the collapse that the building was likely to come down and that everyone should evacuate. Some of them got the message and didn't pay any attention because it didn't come from a source they trusted. The police radio seemed to work fine in that second tower and police officers got the message from their command post to leave the building. As they did they passed the word to firefighters they saw in the hallways. Many of the firefighters didn't leave. They were hearing something from the policemen that they hadn't heard from their command.

The WTC twin towers were located in the down town of New York,. The structure of each of the buildings was basically composed of two major sections: an inner core included the steel columns and outer metal skeleton. The core and outer skeleton were connected firmly to each other through many numbers of special metal links which tied those parts together firmly. Without those links, neither the core nor the outer skeleton could stand up ever. In order to avoid making buildings heavier, all the internal divisions were made from the lightweight (and of course weak) drywall which has a good resistance against fire.

When the twin towers were under design and construction, the trade centre designers tried to anticipate every possible disaster. The towers were the kind of skyscrapers built explicitly to survive the impact of a plane. Leslie Robertson, the head structural engineer of the world trading centre project states: "We had designed the project for the impact of the largest airplane of its time, a Boeing 707, and it is to take this jet airplane run into the buildings, destroy a lots of structure and still have it stand up."

On the September 11, 2001 like on every other business days, at 8.45am the building was busy with around 15000 daily visitors who would normally fill the buildings for their daily works. At 8.46am the first plane hit the North tower. An American Airline Boeing 767, have been deliberately flown to the North tower, striking it across 93 to 98 floors. The aircraft was swallowed up by the building as it hit to the building in 440 mile per hour and had a massive impact on the North tower since it was running too fast and also it was too heavy. There was more than just damage to the outer skeleton. As the aircraft carried on to the building, its engines each weighting four tons, ultimately slammed in to the buildings core (Figure 4.1). The fire then spread at the extraordinary speed because of the fuel the jet was carrying.

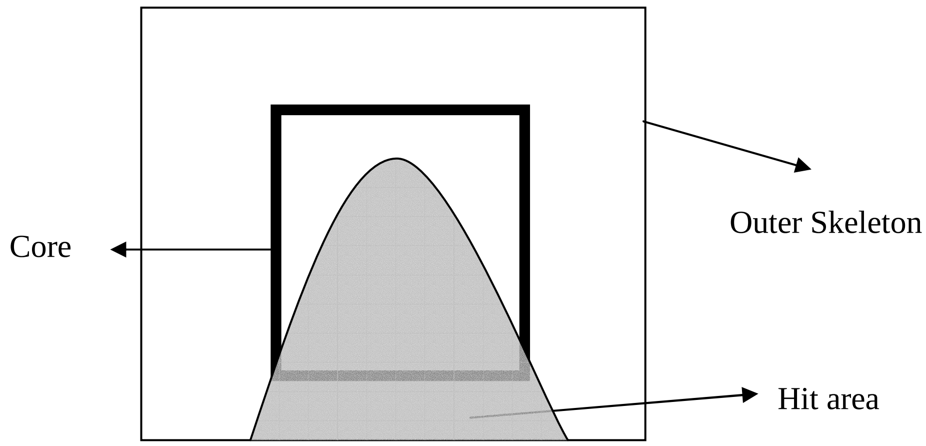


**Figure 4.1** The area destroyed in the North Tower hit by the first airplane (BBC, 2003 )

The jet fuel ignited papers, carpets and plastics and it spread a huge fire across all six floors where the plane had hit. The extent of the fire was something that designers had never anticipated. In this regards, Leslie Robertson states "…with the Boeing 707, to the best of my knowledge, the fuel load was not considered in the design and indeed I don't know how it could have been considered there". The jet fuel caused the fire to spread so far and so fast that it effectively cut the building to two. For the 6000 people below where the plane had hit, the staircases still offered the means of escape but for the 950 people caught above the point of impact on the fire, there was no way out.

What seems to have happened is that fire had flooded into the core and cut off all the stairways, something that should have not been possible, as it should have been protected by the fire resistant drywall. The problem seems to have been that the drywall was not strong enough to protect the escape ways. It seems that drywall responsible to protect the structure against fire around the emergency staircases where the plane hit was simply blown away, allowing fire and smoke to flood into other parts of the building, especially into the floors above the point of impact. That was almost certainly why nearly 1000 people were trapped above the area of impact.

After it hit into the North Tower, the plane dislodged or destroyed many of metal bridges which linked the core to the outer metal skeleton. Those still in place had most of their fireproofing blown off. Most of the inner core columns seems to have survived and still could continue to carry the weight of the building but the fireproofing including the drywall was shattered and without that protection the bare steel of the core was exposed to the intense heat and started to lose its strength and the capability to continue standing firm.

After the first tower was hit by the hijacked airplane many firefighters, police officers and other rescue units got to the scene as soon as they could. But unpredictable problems arose causing obstacles to cope with the huge magnitude of the disaster properly. Any attempt to establish a unified command on 9/11 would have been further frustrated by the lack of communication and coordination among responding agencies. The command posts were in different locations which could have served as a focal point for information sharing and they did not play an integrating role in ensuring that information was shared among agencies on 9/11. There was also a lack of comprehensive coordination between rescue units (Fire Department of New York: FDNY, New York Police Department: NYPD, and Port Authority of Police Department: PAPD) personnel climbing above the ground floors in the Twin Towers. On September 11 2001, information that was critical to informed decision making was not shared among the involved agencies. As a reference to this issue the FDNY chiefs stated that their decision making capability in that morning was hampered by lack of information from NYPD helicopter.

The FDNY chiefs in the increasingly crowded North Tower lobby were confronting critical choices with little to no information. They had ordered units up the stairs to report back on the conditions but they did not know what the impact floors were. They did not know if any stairways into the impact zone were clear. They did not know whether water for firefighting would be available on the upper floors. They also did not know what the fire and impact zone looked like from the outside.

### 4.2.3 Second hit on the World Trade Centre

At 9.02am the second airplane hit the South tower, impacting between floors 78 to 84. The plane had sliced into the South tower at an angle to the right. Unlike the North tower it missed most of the core and thereby smashed the eastern wall. (Figure 4.2)

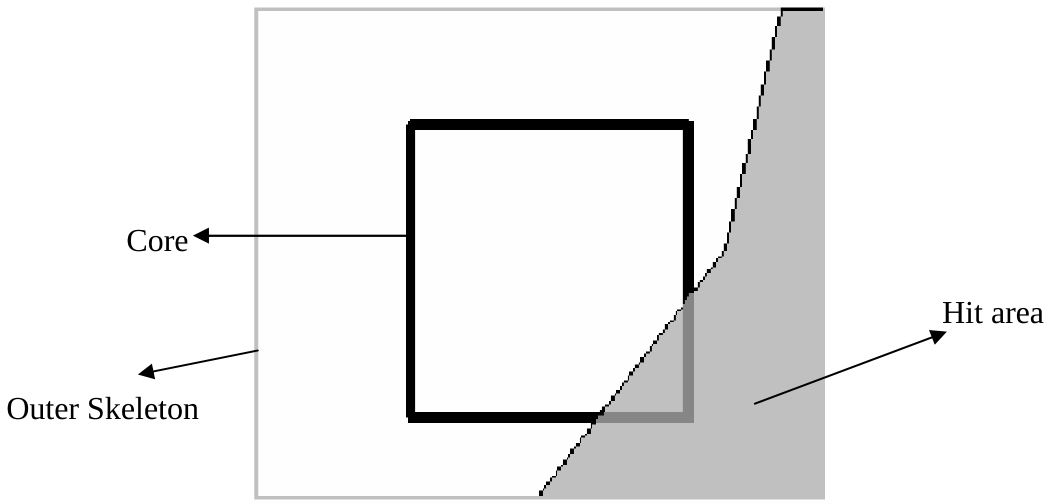


**Figure 4.2** The area destroyed in the South Tower

hit by the first airplane (BBC, 2003)

Initially the South tower responded well and seemed capable of standing but in one vital respect it had been hit in a more critical place than the North tower. It had been struck lower down which meant that the damaged structure had to bear a much heavier load. Inside the tower the plane had again destroyed some of the metal links between the core and the outer skeleton and stripped the fire protections off the others. Though the core had not been hit so badly, much of its protective drywall had been shattered and again stairways and lifts were exposed, allowing the fire to spread. At this stage about 2000 people left alive in the South tower, some 1500 below where the plane had crashed. Just as in the North tower these 1500 people still could make their way down. For the 500 left above the impact line, two of the three staircases were completely impossible and one still offered the way out in its minimum capacity due to the heavy smoke and fire.

Almost immediately after the South Tower was hit, senior FDNY chiefs in the North Tower lobby asked the others to discuss strategy for the operations in the two towers.

Of particular concern to the chiefs was communications capability. One of the chiefs recommended testing the repeater channel to see if it would work. Earlier, an FDNY chief had asked building personnel to activate the repeater channel, which would enable greatly-enhanced FDNY portable radio communications in the high-rises. One button on the repeater system activation console in the North Tower was pressed at 8:54 a.m. As a result of this activation, communication became possible between FDNY portable radios on the repeater channel. In addition, the repeater's master handset at the fire safety desk could hear communications made by FDNY portable radios on the repeater channel. There was a second button that needed to be pressed for the activation of transmission on the master handset. That second button was never activated on the morning of September 11.

At 9:05 a.m., FDNY chiefs tested the WTC complex's repeater system. Because the second button had not been activated, the chief on the master handset could not transmit. He was also apparently unable to hear another chief who was attempting to communicate with him from a portable radio, probably because of some technical problems. Because the repeater channel seemed inoperable since the master handset appeared unable to transmit or receive communications, the chiefs in the North Tower lobby decided not to use it. The repeater system was working at least partially, however, on portable FDNY radios, and firefighters subsequently used repeater channel 7 in the South Tower.

At 9:51 a.m., a helicopter pilot cautioned that "large pieces" of the South Tower appeared to be about to fall and could pose a danger to those below. Immediately after the tower's collapse, a helicopter pilot radioed that news. This transmission was followed by successive communications at 10:08 a.m., 10:15 a.m., and 10:22 a.m. that called into question the condition of the North Tower. The FDNY chiefs would have benefited greatly if they had been able to communicate with personnel in the helicopter.

57 minutes after the second attack, At 9.59 a.m. the South Tower collapsed due to the heavy load it was bearing and the intense heat weakened the bare steel of the outer skeleton. In addition, the loose connections between core and outer skeleton accelerated this process since many of the links between the core and the outer skeleton were demolished by the impact. It took only about 30 seconds for the tower to collapse entirely and 600 people died in this tower, 500 of them were those trapped above the point of impact.

At 10.03 a.m., four minutes after the first tower collapse, there was now one terrible implication. If the South Tower had fallen, the other one was likely to follow. An urgent message was radioed to all firefighters and policemen in the North tower: "Evacuate the building immediately." The South Tower's total collapse was immediately communicated on the dispatch channel by an FDNY boat on the Hudson River; but no one at the site received this information. Despite his lack of knowledge of what had happened to the South Tower, a chief in the process of evacuating the North Tower lobby sent out an order within a minute of the collapse: "Command to all units in Tower 1, evacuate the building." Another chief from the North Tower lobby soon followed with an additional evacuation order issued on tactical channel 1. A group of firefighters (the ladder 6) from the NYFD were on the 27 floor at that moment. Mike Meldrum (BBC, 2003) a ladder 6 fire crew of NYFD states "We heard somebody yelling on the radio that it's time to stop and back down now". Within minutes, some firefighters began to hear evacuation orders over tactical channel 1. At least one chief also gave the evacuation instruction on the command channel used only by chiefs in the North Tower, which was much less crowded.

Many FDNY personnel in the North Tower who received the evacuation orders did not respond uniformly for several reasons. Also a number of FDNY personnel did not hear the evacuation order on their radio but were advised orally to leave the building by other firefighters and police who were themselves evacuating.

25 minutes later at 10.28 a.m. still nearly 1000 people were trapped in the upper 20 floors, plus many firemen unaware of the evacuation order and still inside the tower were trying to save people. At this moment the North Tower came down. The theory is that the main reason for the North tower to collapse is that the tense fire had weakened the bare steel of the core columns and this had caused the building to start pancaking down similar to a situation in controlled structure demolishing.

In total 2800 people died in the attack, 479 of them were from the emergency services including 343 firefighters.

## 4.3 Case Discussion

This section outlines the numbers of considerable communications problems that took place in the WTC on the September 11, 2001 resulting in many firefighters' fatalities. Among the many problems, those related to sharing important information and also wireless radio interruption and unavailability seemed to have significant impacts on the firefighters’ lives.

The September 11 WTC collapses and its consequences on the rescue crew fatalities bring to attention the fact that the traditional communication systems and commercial wireless equipments that were used by the firefighters did not respond properly to the dynamic environment. Communication systems became overwhelmed by the huge amount of different data traveling throughout the network. The US 9/11 Commission Report (2004) made a comparison between the number of NYPD and FDNY casualties and deaths. The report clearly states that the success of NYPD instruction can be credited to a combination of:

- The strength of the radios they were using
- The relatively small numbers of individuals involved in the scene
- Use of the correct communication channel used by all individuals

Also the report stresses that the same three factors worked against successful communication among the FDNY personnel.

- First, the radios' effectiveness was drastically reduced in the high-rise environment.
- Second, Initially all the FDNY units were using the tactical channel 1 for the communications purposes, so this channel was simply overwhelmed by the number of units attempting to communicate.
- Third, some firefighters were on the wrong channel or simply lacked radios.

Also wireless equipment used on the WTC case caused an obstacle against reliable communication. Public safety personnel regularly use cellular phones, personal digital assistants (PDAs) and other commercial wireless devices. As previously mentioned through the review of literature, these devices are not sufficiently suited for public safety mission-critical communications. As researchers involved in the Commtech Agile project (2003) describe, public safety cannot depend on commercial systems that can be overloaded and become unavailable. They stress that experience has shown such systems are often most unreliable during public safety operations. Rescue operations have unique and demanding communications critical to handle the incidents and public demand overwhelms the communication channels and systems.

Also this case reveals that there was a significant impact on the firefighters' communications when communications in the North Tower were redirected to the repeater channel after 10:00 a.m. to resolve the congestion problem. This repeater was considered as the focal system which would handle the communications throughout the North Tower. However, according to the US 9/11 Commission Report (2004) that system should start and be managed manually and it is not clear whether the repeater channel continued to be operational after 9:59 a.m. This make clear that after 9.59 a.m. not only all the communications from firefighters teams to senior chiefs were cut, but also any inter-communication among team crews and team members were no longer available since the repeater as the backup system became the single point of failure for the communications purposes.

Another problem encountered that seems to have had a considerable impact on the firefighters' lives was the inconsistency of vital information among different groups due to lack of interoperability and its consequences on the senior commanders' decisions. Despite the fact that many police officers received the evacuation warning and saved their lives, many firefighters remained within the North Tower unaware of the serious threat of tower collapse. Looking at the case carefully it is clear that radio communications were a lifeline for the hundreds of police officers who received the word to evacuate the building. Evidence and reports show that all 60 police officers escaped with their lives.

Tragically, hundreds of New York firefighters didn't receive that warning because they were using a different radio communications system. As the Agile research group at Commtech (2003) cited in a report from the University of New Hampshire-based, ATLAS Project "From numerous interviews gathered as part of a fire department inquiry into the events of September 11th, it would appear that non-interoperability was at least partially responsible for the loss of 343 firefighters at the World Trade Center." This was a considerable issue on the day of the September 11, that there was no adequate and reliable interoperability among the different groups involved in the rescue operation and civilian evacuation. As the result of this problem the information sharing suffered. There was a lot of redundancy and conflicts of the tasks and lack of cooperation among different parties due to disparity and inconsistency of the critical information. These problems had posed a serious impact on the overall performance of the rescue operations since commanders couldn't make a united decision and take coordinated actions.

Evacuation orders did not follow the protocol before the North Tower collapse. The US 9/11 Commission reported (2004) that giving instructions when a building's collapse may be imminent follows a standard protocol including constantly repeating "Mayday, Mayday, Mayday". During the 29 minutes between the fall of the South Tower and that of the North Tower this message had been never sent to the firefighters. In addition, most of the evacuation instructions did not mention that the South Tower had collapsed. This issue could be considered as the human fault under the high pressure. Furthermore, the problem could have been made worse by the communication systems which were unable to integrate the standard protocols and communication features to reduce the impact of wrong decisions.

Furthermore challenges concerning the lack of the ability to disseminate the critical information throughout a reliable network were remarkable on the WTC case. It seems that communications networks were unable to operate simply in a high pressure environment and they couldn't handle the crucial information in each direction. As a reference to this point, US 9/11 Commission (2004) reveals that firefighters did not receive the evacuation transmissions, for one of four reasons:

- First, some FDNY radios did not pick up the transmission because of the difficulties of radio communications.
- Second, the numbers trying to use tactical channel 1 after the South Tower collapsed may have drowned out some evacuation instructions. According to one FDNY lieutenant who was on the 31st floor of the North Tower at the time, "[Tactical] channel 1 just might have been so bogged down that it may have been impossible to get that order through."
- Third, some firefighters in the North Tower were off-duty and did not have radios.

- Fourth, some firefighters in the North Tower had been dispatched to the South Tower and likely were on the different tactical channel assigned to that tower.

## 4.4 Case Study Analysis

The following section outlines how the application of mobile agents and new wireless technology can bring new values to the public safety operations and how it can be valid in public safety rescue tasks. This section includes the criteria selected to aid in determining the most important changes that might happen to the communication system through the application of mobile agents and wireless technologies. In addition, this section will discuss the outstanding communication issues that were raised in the case of WTC fall and it attempts to analyse each problem based upon the considered criteria. It also will analyse the ways that mobile agents and wireless technology could help in public safety operations to cope with the perceived problems and it will analyse the evaluation criteria.

As the Commtech Agile project research (2002) outlines, an optimal public safety radio communication systems require satisfying five primary criterion:

1- Dedicated channels and priority access that is available at all times.
2- Reliable one-to-many broadcast capability.
3- Highly reliable and redundant networks that are engineered and maintained to withstand natural disasters and other emergencies.
4- The best possible coverage within a given geographic area, with a minimum of dead zones.

5- Unique equipment designed for quick response in emergency situations since in critical events seconds can mean the difference between life and death.

If the above criteria could be met then it would provide a communication system attractive for public safety tasks. Such a system is being introduced by Marstrander & Hanssen(2002) as they describe that the public safety officials need to own communication systems which could provide them with the ability to make a complete, accurate, and timely information sharing to complete successful operations. The research through this thesis, attempts to add another measure to the mentioned criteria. This criterion is the communications systems' ability to make some processes on the travelling data and correspondingly make some local decisions based upon the local data travelling throughout the system. These local decisions made by the system aim to facilitate the human decisions to be made in more reliable ways and timely fashions, particularly in the highly dynamic environment. In fact, this characteristic is a degree of intelligence and autonomy that could be embedded and merged into the systems by the mobile agents and the wireless network which support them.

From the communication perspective, looking at the main issues affecting the firefighters and commanders in the WTC collapse, the following section highlights and discusses such issues. In particular, it discusses to what extent the wireless technologies and mobile agents could solve or alleviate these problem.

### 4.4.1 Large number of users involved in the radio communication

As the case study reveals, on the September 11 rescue operations, one reason that negatively affected the firefighters' ability to communicate with each other was the large number of the firefighters who were present on the scene. This issue had affected the reliable one-to-many broadcast capability of the firefighters' communications systems due to their communication systems limitations.

Traditionally every radio communication system has limited capacity for delivering messages. In fact, communication systems performance is highly dependent on the number of users using the network at the same time. This makes the network bandwidth a rare resource since every user shares the whole bandwidth to send and receive their messages. This becomes a significant issue when the public safety workers plan to use their radio communication systems which are being congested by the large number of users on the scene. Some experts like Smith and Tolman (2000) suggest that public safety systems could use the commercial spectrum for their radio communication purposes. Although it would work in many situations, in the events that have a considerable impact on the large number of civilians, commercial radio spectrum could also be congested since civilians will occupy the large amount of bandwidth for personal reasons. One promising solution to this issue that has potential for public safety use is the mesh networking technology.

According to Walker (2004) mesh networks are based on the concepts of mobile ad hoc networking. They are known as the networks formed by users or devices wishing to communicate, without the necessity or existence of any previously infrastructure established between the potential network members. Mesh networks can take place in different scenarios and are independent of any specific device, wireless transmission technology, or network protocol. They can significantly vary in size depending on applications. Based on the literature, mesh networks are able to adapt to the dynamic environment since they are self-healing and self-configuring. Also they can accommodate a large number of users because each mobile device is a part of infrastructure and network routing system.

As Schoen (2002) describes, mesh networking technology has been initially designed and exploited for the military purposes and it has shown significant advantages over other networking topologies for the on field communications in terms of capacity and the number of users who can communicate with each other at the same time. Also, as Schoen (2002) highlights the general advantages and specifications of mesh networking for public safety use, including the fact that this configuration is highly flexible in handling the varying number of mobile users. This situation might happen in public safety rescue operations like that of September 11, 2001. As a result, wireless radio technology that could work properly in a mesh configuration would be interesting to many public safety rescue tasks, especially where the large numbers of crew are involved. It could support a small or large numbers of users in a given geographical area. Also it is a promising technology to handle the one-to many and many-to-many communications in a reliable and flexible means. Mesh technology can help public safety communications to achieve the compromises between the number of required crew for the rescue tasks and the required communications capacity.

### 4.4.2 Lack of interoperability among different parties

One considerable issue in the September 11, WTC fall was the interoperability problem. Smith and Tolman (2000) describe the interoperability in the context of public safety as the ability to share information in real time between agencies who are involved in the operation. Basically it means that persons who need to exchange information should be able to do so, even when they are using different technologies from different manufacturers. In the broader definition from Smith and Tolman (2000) interoperability refers to the ability to transmit all types of communications electronically, including voice, data, and images.

Research carried out by the Agile project at Commtech (2002) describes the number of primary issues that are obstacles to the public safety interoperability. Among those "Diversity and incompatibility of the contemporary network devices used in the public safety" is the one more interesting to this research since it focuses on the interoperability challenges which have root in the network devices. The other four issues discussed by them mostly refer to the challenges concerned with the funding, governmental decisions and project managements and planning.

In fact, diversity and incompatibility of the contemporary network devices used in the public safety has considerable impact on public safety interoperability since it significantly affects the definition of the interoperability and its characteristics as described by Smith and Tolman (2000). Lack of interoperability can weaken the ability of public safety operation to respond properly to the dynamic situations. This means that communication systems are not able to cover the necessary area since the public safety equipments cannot communicate with each other.

Mobile agents show a promising solution to this issue as Lange and Oshima (1999) express that mobile agents in a distributed communication system naturally act heterogeneously. In fact, communication networks and computing are fundamentally heterogeneous, both from the hardware and software perspective. Lange and Oshima

(1999) describe that mobile agents are generally independent of any computer platform and network transport layer and their performance only depends on their execution environment. This means that they can provide the optimal condition for the seamless system integration which significantly could help to make a reliable inter-links between different communications systems used in public safety. Another unique characteristic of mobile agents is their ability to encapsulate communication protocols. According to Lang and Oshima (1999) in a distributed system, as protocols evolve to accommodate new requirements for efficiency or security, it is cumbersome if not impossible to upgrade protocols properly. Consequently, communication protocols often become a legacy problem causing an obstacle for establishing interoperability among different systems and devices.

White (1996) provide a solution to this issue by explaining that mobile agents can move to remote hosts to establish communication channels based upon proprietary protocols. This means that a mobile agent can establish a channel between two network nodes where each node may rely on different communication protocols. In fact, regardless of the size and strict requirements under which communication networks operate, mobile agent technology can function as the glue keeping the systems flexible and effective.

### 4.4.3 Data traffic and network congestion

In the case of WTC fall, communication networks experienced a number of technical problems. One important challenge that undermined their performance was the data congestion and high network traffic throughout the networks. Network congestion can seriously affect communication network performance. As McCabe (2003) describes "capacity" is a class of performance characteristics of a network involving the moving of information from place to place within the network and it includes bandwidth, throughput and so forth. When the network traffic starts rising up then the network bandwidth will be less available for handling more information. As a result, there would be compromises between the network service availability and the amount of data that can travel throughout the network. As the case study shows, this problem highly damaged the communication reliability, coverage area and responsiveness.

Pham and Karmouch (1998) state that much research into mobile agents has two general goals: reduction of the network traffic and asynchronous interaction. These applications of mobile agents remarkably could be also useful to public safety communications. As the case study reveals, network congestion has an undeniable effect on the rescue performance. In fact, mobile agents allow users to package a conversation and dispatch it to a destination host where interactions take place locally. This is what Lang and Oshima (1999) describe as the mobile agents' ability to reduce the network load in a distributed system which relies on a communication protocol. Furthermore, they believe that mobile agents can be used in critical real-time systems since they can be dispatched from a central controller to act locally and execute the controller's directions directly.

Another potential solution to the issue of the network congestion is the new wireless technology such as ad hoc mesh networking which can support high bandwidth network configurations. As Broersma (2004) explains each device on a mesh network receives and transmits its own traffic, while acting as a router for other devices. Intelligence in each device allows it to automatically configure an efficient network and to adjust when, for example, a node becomes overloaded or unavailable. According to Broersma, the advantages include ease of setup, the ability to spread wireless access over a wide area from a single central wired connection and the inherent toughness of such networks.

So, in public safety operations where in many situations the environment is highly under pressure and any changes would happen very fast, having a communication network that could handle crucial information with the less possibility of congestion problem is vital. Mobile agents and new wireless technologies show encouraging potential to handle this issue for the public safety purposes.

### 4.4.4 Lack of Meta Data

Passing of information from one person to another, with understanding, is the fundamental purpose of any communications system and interpersonal communications normally include more than just verbal exchanges. Tone of voice, body posture, and eye contact all are part of everyday communications. As Marstrander & Hanssen (2002) state, emergency communicators usually don’t have the luxury of using all of these elements that make up interpersonal communications. Their communications are limited to what is spoken or heard and a well trained emergency communicator and appropriate listening skills are critical for successful communications.

In other word, some other data that could give complementary information about the primary information is critical to the rescue operation and crews' lives. This data could be collected and interrupted locally via mobile agents through the communication with other agents or sensors residing on the agents' hosts. Mobile agents can sense users' environment through the sensors interface between agents and environment. In fact a sensor network could sense some critical elements of the physical environment (Boukerche et al., 2004) such as body temperature, blood pressure or speed and direction of the wind and pass this information to the agent waiting for that data. Agents can carry some processes or deliver raw data to the appropriate place in the network. Sensor networks could be setup as mesh configurations and cover a broad geographical range of environments. This complimentary data could be used significantly as the raw data itself or metadata to make the communications more sensible and reliable for the senders and receivers.

Lang and Oshima (1999) describe this application of the mobile agents as the "Monitoring and notification" application and identify it as a classic application of the mobile agents based on their asynchronous behavior. As they explain, mobile agents can monitor a given information source without being dependent on the system from which it originates and they can be dispatched to wait for certain kinds of information to become available. So, agents could be programmed to act as thresholds and make corresponding processes or generate proper messages based on the sensing situation. This combination of sensor networks and mobile agents could bring new kind of data available to users that are not generally accessible to decision makers through the traditional communication systems.

### 4.4.5 Network interruptions and volatility

One important issue encountered through the case study is the frequent network breakages because the network was overwhelmed by the users or due to some technical problem such as communications infrastructure damages. One way to deal with this issue can be found through the unique specifications of the mobile agent. As Wooldridge and Jennings (1995) describe, agents are generally autonomous, reactive and, adaptive to their environment. This means that agents can sense their execution environment and react properly based upon their tasks and the environment. Also they have the ability to dynamically adapt with their environment in order to gain the best performance. Lang and Oshima (1999) justify this point by stating that mobile agents are robust and fault tolerant. They endorse the idea of making a robust and fault tolerant distributed systems on top of mobile agents since in a given distributed system, mobile agents have the ability to react dynamically to unfavourable situations and events.

To back up this idea, Milojicic (1999) cites from Kotz that mobile agents will most likely be useful in situations where networks face frequent disconnections, such as wireless devices which frequently get disconnected from the network. Kotz (cited in Milojicic, 1999) adds that mobile agents can handle network disconnections by keeping their state and data and deliver the data to its destination after the connection is established again.

This characteristic of the mobile agents make them capable to move throughout a wired of wireless network and make a considerable contribution in reducing the undesired effects of the network disconnections. This ability becomes more crucial when the network is responsible for delivering important and life sensitive information from the source to its destination. In agent-less networks when the network breaks during the transmission process, the whole data and required processes should be resent to the destination later again. However, agents can distribute throughout the network and continue performing their tasks on their hosts even in the absence of network connections. Also they can keep their states and processes results until the network becomes available to transmit their data. These are the features that will significantly improve network reliability which is crucial for public safety operations.

Another way to cope with network volatility and to make the network flexible against disconnections is the use of network setup that could facilitate changes. Again one promising approach is to use mesh networking setup.

### 4.4.6 Problems concerning the suitability of equipment

The public safety field has suffered from the lack of having proper equipment designed specifically for their special missions. The US National Institute of Justice guide for the Selection of Communication Equipment for Emergency First Responders (2002) discusses this issue by emphasizing that public safety workers use commercial equipments in order to accomplish their task. But the problem with this equipment is that it is not designed for public safety mission-critical assignments. Also they add that many of this commercial equipment is not physically and functionally fit to the extreme and dynamic environment where public safety workers perform their tasks.

According to Evan et al., (2002) personnel in military and civilian emergency situations must have completely unhindered mobility. On the other hand, they should be armed with as much information and data as they can effectively utilize. So they require to be equipped by systems which are flexible and reconfigurable and fit to their special requirements. Child (2003) describes one such device which a foot soldier can wear in order to improve his situational awareness, lethality and survivability. Through these systems and equipment soldiers can view maps and orders, view known enemy positions and they know literally where they stand in relation to other squad and platoon members.

Networking of wearable computers is another area where many technologies are playing an expanded role. According to Child (2003) the traditional network schemes cannot work when a huge amount of data travels through the network and when a large number of users are using wearable computing devices in order to accomplish their missions. Child (2003) states that the in a situation where 5000 soldiers and vehicles report back to central command, a hub network environment is far from practical and an ad-hoc, self-configuring multi-path network makes more sense.

With reference to the WTC case, this situation might happen in many public safety rescue tasks and public safety workers need to be equipped with devices which can sense many environmental information. Additionally, information from these devices should be passed through a reliable network which can handle high traffic. Again, a combination of mobile agents and new wireless technologies could offer a good solution to this issue. These technologies could combine with the wearable computing devices in order to help public safety crew access valuable information about their environment to make local decisions or relay that information in a reliable manner to other places in the network where they are needed.

### 4.4.7 Intelligent communication systems with autonomy

Public safety communications through the radio systems rely primarily on voice communication and they are designed to convey voice in the best way possible. But these systems do not have any features that make them capable of sensing their environment and perform some processes and decision making based upon the perceived situation. This is a shortcoming that has not been discussed throughout the literature.

As discussed earlier, this idea could help public safety workers not only become more aware of their situation locally but also it would help decision makers have a broader sense of the overall picture of the operations on the field. Essential for these systems is that they should be authorized and capable to act autonomously. Also they should be able to establish a relation with their environment and perform within their environment proactively and reactively. This capability could be translated to the degree of systems' intelligence in order to integrate and transfer many of the human tasks to the systems functions. In such a system, many decisions would be made locally.

As Lang and Oshima (1999) spell out, in many situations it is more efficient to move the small computation and required processing to the place of the large volume of the data rather than move the data to the computation place. The local computing could be any kind of processes that would affect the local situation in terms of grabbing and producing new local information, filtering the unnecessary data, generating complementary information based on the protocols and so forth. With reference to this idea, as the case study reveals, before the North Tower collapsed, a number of firefighters who received the evacuation order did not respond properly since the order did not follow the standard protocol and they did not trust what they were hearing. Consequently they did not put the evacuation order in their priority.

A parallel and complementary system providing them with supplementary information about their situation or hazards could be used as a benchmark helping them to get more aware of their situation. Such a system would encourage firefighters to pay more attention to the announced warning. Such information would also be valuable for decision makers as discussed in the previous sections.

Any system, including communication systems, in order to act intelligently should have specific capabilities and characteristics. Fritz (1996) defines “intelligence” as the system's level of performance in reaching its own objectives. He states that a system with greater intelligence can reach its objectives sooner or faster compared with other systems in the same situation. Fritz (1996) also spells out that an intelligent system could not function unless it had senses, a method to choose responses according to its objectives and some way of performing these responses in and on its environment.

As discussed earlier, mobile agents, new wireless technologies and the proposed equipment could help public safety officials to cope with the perceived issues discussed above. In addition, these technologies will make the communication systems more intelligent. In fact, taking advantage of the mobile agent technology and merging their attributes to the communication system, will make these systems more interactive with their environment in more meaningful ways. Agents generally tend to sense and interact with their environment based on their specific goals and objectives. These objectives and the practical ways that mobile agents could interact with their environment are discussed in detail by Wooldridge and Jennings (1995).

In addition to mobile agents, wireless mesh networking is a technology that could bring a degree of intelligence to the communication system. Since this technology is a highly flexible technology which can adapt to the changing networking environment, it would make communication systems more adaptive and intelligently responsive to the network load to gain the optimum traffic balance.

In conclusion, applications of mobile agents and new wireless technologies not only can help to overcome or alleviate the discussed problems but they will also add a degree of intelligence to the communication systems making them interactive with their environment in order to gain the best performance in the timely and reliable fashion.

These conclusions lead us to apply the outcome results of this case study (secondary case study) in a real world situation.

The following chapter will discuss the technologies that could contribute in the public safety domain in order to assist the involved party for better and more reliable situation awareness, decision makings and corresponding action. It is in the favour of this thesis to have more accurate and deeper look onto the available and potential technologies that could contribute in this area. Also human role as the key player of the critical decisions and action will be investigated in the following sections

# Chapter 5

# Discussions

## 5.1 Introduction

As shown by the case study described in the previous chapter, public safety tasks and their operational environment are characterised by ambiguity, high stress, and time dependency of decision-making. The decision-making process follows a distributed pattern where mobile team members with different skills are distributed across a networked operational environment. They must make decisions to act with incomplete and inaccurate information about their environment. In this situation, high quality computer support is critical (Payne et al., 2000) to integrate the human and technical capability.

Recently, the technology of software agents has emerged as a suitable metaphor for representing the computer processes that assist human decision-making. Such software agents should not only retrieve information on request; but they should actively and intelligently anticipate, adapt and actively seek ways to support users (Bradshaw, 1997). In addition, they can reduce the amount of interaction between humans and the computer system and allow the humans to concentrate on other activities, such as assessing the situation, making decisions, or reacting to changes in the system (Zachary et al., 1996). This timesaving is critical in the situations described in this thesis.

To provide a holistic and balanced view of the problems and possible improvements to coordinated responses to emergencies and disasters, human aspects of the situation also need to be understood. To address the human side a discussion is made of the issues of situational awareness and sense-making that affects human-decision making to take action in high stress and time-critical environments. The critical observation is made that developing technological solutions without understanding these concepts is futile.

This chapter concerns the ways that different technologies such as mobile agents and wireless technologies support human decision makers to cope with uncertain threatening environment. The chapter is arranged as follows: The following section will borrow a military model of users call Small unit operation (SUO) and explains how it could be suitable for other public safety agencies and tasks. Following that, there will a comprehensive discussion about the mesh networking topology as the preferred network topology that could be appropriate to the requirements rescue and emergency operations. Characteristics of different radio technology, especially Ultra wideband will then be discussed in order to determining the most promising wireless radio technology that would take the responsibility of radio communications. Then sensor wireless networks will be presented and discussed as a real and available technology which can embrace and work with the other technologies involved. At the conclusion of the chapter a complementary and focal discussion will be conducted regarding the key attributes of humans in the collaborative decision-making processes leading to effective actions in critical situations and dynamic environments.

## 5.2 Small Unit Operation

Small unit operation is an arrangement of people and tools proposed by the US Defence Advanced Research Projects Agency (DARPA). It aims to accomplish tasks in a fast changing environment effectively (DARPA 2004). In a small unit operation people and equipments work cooperatively in a dynamic and even extreme military environment in order to accomplish specific tasks. It is described by DARPA as a situational awareness system with the objective of supporting communications among the mobile entities (human and equipments) with high data rate capacity that is optimized for restrictive environment.

According to Brown et al. (2004) the small unit operations is a configuration of people and equipments who work together to meet some mission objective. In a SUO, entities have distinct roles and also specific information needs and they are often distributed geographically. In fact, the small unit operation includes teams of inter-communicating people and autonomous entities such as military troops, police, firemen, rescue workers, vehicles, sensors, and so on.

SUO mission types can include any collection of tasks and subtasks coordinated to achieve a mission objective. For example mission types could be search and rescue, evacuation, clear minefield, relief, and others (Brown et al., 2004). In this sense, because SUO heavily relies on the mobility and communications in dynamic environments, the key component to the effectiveness and success of the SUO, is the reliability and operativeness of communications system. These communications systems should support the availability of the required information for the SUO participants at the right time in the right place.

Although the SUO model is initially proposed to support military tasks, but it also fits other kind of tasks which naturally have the basic requirements whose operational environments are similar to SUO military environment described by DARPA (2004). Therefore, public safety operations can also take advantage of the capabilities of the SUO model in order to improve its communications hurdles discussed earlier. This is what Brown et al. (2004) describe as the ability of the SUO system to be extensible for other mission, roles and scenarios. Furthermore, McGrath et al. (2000) propose an agent based communication system build on the top of SUO model and they stress that their system can be applied to other domains that have characteristics similar to the military applications. These characteristics include constraints on network reliability and bandwidth; domain-dependent information processing; and complex, autonomous information processing involving large heterogeneous data resources.

Traditionally in military and public safety, communications take place through radio systems by passing verbal messages. Of course this type of communications has some advantages since radio permits two-way responsiveness; multi parties can monitor radio communications; parties could convey emotions during the transmission; and the use of radio is well tried, tested and familiar. So every other proposed communication system should not aim to replace radio communications system, rather it should try to augment it. According to Brown et al. (2004) the potential areas where the SUO communication system can assist radio include: controlling the avalanche of information; many people can speak at once; store information over time; memory aid; listening aid; support for disconnected operations; assured delivery; accuracy; auto create and auto handle messages; after action analysis; and stealth.

Brown et al. (2004) also propose a communication system to support the SUO. As they argue the system could meet top level requirements such as: automated data capture, mission and role specific data acquisition, intelligent processing, and custom task and role centric information filtering and display, as well as access to remote information sources. Also it could support the architecture that consists of agents communicating grid. Furthermore their system will operate on a computing device to support mission planning and potentially on a smaller footprint hardened hardware platform to support mission rehearsal and execution. These requirements are fairly close to the requirements of the firefighters and other public safety agencies during their missions.

## 5.3 Mobile Agents

As discussed earlier, mobile agents have specific characteristics that enable them to be applied in dynamic and volatile environments in order to deal with communications problems and network connection failures. These abilities have roots in mobile agents' attributes such as autonomy, adaptively, persistency and so on. According to McGrath et al. (2000) mobile agents provide an excellent mean of meeting critical requirements for many military and civilian applications, particularly those in which low bandwidth or intermittently connected networks or both of these problems are present. Agents are also useful tools when information to be discovered and processed resides in heterogeneous, distributed resources. They also explain that mobile agents fulfilled an important requirement on the SUO communication system such as robust information dissemination across unreliable networks. These typical applications show that mobile agents are the proper option to deal with many sources of uncertainties in a dynamic environment such as public safety or military operation environment.

McGrath et al. (2000) also express the number of challenges that military and civilian systems are face with them. These issues make systems less effective and less responsive to the specific military tasks. Among them, the challenges of using stove pipe systems and high amount of information retrieval and analysis in short period of time, are outstanding. As the consequences, people are in the process between complex systems and when the people became too overloaded, valuable information is unavailable when it would be most useful.

So, mobile agents' can help to fulfil the military and civilian operations requirements in order to overcome the mentioned challenges. As McGrath et al. (2000) explain, application of mobile agents that can fit to the following situations:

1- Information retrieval, dissemination, monitoring. This functionality has been effectively achieved by the mobile agent technology. Such agent-based systems will be most effective if they can be implemented as extensions to systems that are already in use, eliminating the requirement for already overloaded operators to learn more new information systems.

2- Heightened efficiency at low bandwidths. Mobile agents can make an enormous impact on low-bandwidth in military or public safety networks because they can analyze and filter data at its source, thus reducing the amount of bandwidth required to execute a task. This is particularly relevant to networks in the operation fields since networks at headquarters and command and control units tend to be fairly high speed but communications links to in the front lines and event scenes tend to have much lower available bandwidth.

3- Robust performance on intermittently connected networks. Wireless networks often form the basis for deployed, team member communication and such network connections frequently fail as team members move out of range. Because mobile agents are able to persist at a node, even without a fully connected network, they provide a robust level of fault tolerance in unreliable networks (Lange and Oshima, 1999).

So it is critical to have or design a number of mobile agents that can handle the mentioned tasks. In order to fulfil the requirements of those tasks, McGrath et al. (2000) have developed an agent base system based on three capabilities of mobile agents coupled with the SUO military tasks: Information push, where mobile agents automatically send information to other agents or entities that may need it; Information pull, where mobile agents retrieve relevant information from distributed sources; and Sentinel monitoring, where one or more agents persistently checks for an event or existence of a condition and reacts to its occurrence.

These applications of mobile agents can properly be applied to the public safety tasks since they are based on the SUO model and dynamic environments. Because they can be fitted well to the particular requirements of public safety operations such as constraints on network reliability and bandwidth; domain-dependent information processing; and complex, autonomous information processing involving large heterogeneous data resources(McGrath et al., 2000). In this sense, considering the similarities of public safety and military operations environment and requirements, mobile agents are proper choice to act in an emergency first respond task based on the SUO model.

In the public safety tasks, every brigade or team could be considered as a SUO, and agents could be applied to assess the situations, disseminate information among the deployed units and their members. For example, firefighters in the field may receive reports, signals or data from sensors they are wearing and may generate reports based on their own observations. These critical information need to be rapidly collected from every team member and be sent to the other members and as well as the commanders above for the further and quick decision makings. This could happen based on the assigned priority to the information and priority of the destination who may need this information. In order to minimize load over the low bandwidth network, agents can analysis and determined which members in the team required a given piece of information.

This assessment and analysis could be made primarily based on location constraints and the mobile agents could deliver the reports to the recipients based on specific criteria e.g. their geographical location or their rank. Also, the mobile agent can handle connection failures by retrying at intervals, then informing the sender the situation of the connection upon unrecoverable failures.

Agent, and specifically mobile agents, could also be used to facilitate distributed information retrieval (McGrath et al., 2000). Systems can use mobile agents to query heterogeneous databases over intermittently connected and low-bandwidth networks. It significantly reduces information dissemination and retrieval latencies, enabling decision makers to radically improve the reliability of their analyses. Practically, mobile agents that move from a moving entity (soldier, firefighters, vehicle…) into the main network perform all multi-step queries. The agents interact with the required databases without using an unreliable, low-bandwidth link to connect the moving node to the main network. The mobile agent can complete the query faster, and does not waste bandwidth by sending intermediate results back to the requester (White 1996).

With this capability, decision makers could avoid exhaustive searches of all data sources. According to McGrath et al. (2003) they search instead the 2% (average) of sources that are actually relevant to the query. This is an advantage that could help decision makers to make agile and effective decisions especially those that heavily rely on data and information stored in the databases applicable to a specific issue.

One important task in the military and public safety operation is the contingency planning. According to McGrath et al. (2000) contingencies for critical emergency operations take priorities and may be planned only a few moments in advance. In this situation mobile agents can persistently monitor distributed data sources for potential dangers. Afterward mobile agents would be used to perform analysis in order to determine if a danger or thread actually occurred, and then alert decision makers and team members regarding the analysis results. So, they could re-plan the mission to avoid the danger. As McGrath et al. (2000) express, in this situation users are able to passively monitor critical data sources and automatically receive relevant alerts, thus eliminating the need for the user to be constantly involved in time consuming and lengthy data searching tasks. Also Gray (2000) explains that mobile agents are important tools to deal with time consuming software installation since they eliminates the need for the pre-installation steps, something that is important if the mission is planned or changed rapidly.

These applications of mobile agents along with the specifications of the SUO model could significantly help the public safety operations to get deal with their risky tasks in more reliable means. The way mobile agents could handle the task in terms of retrieving the critical information, making alerts, handling the wireless network issues and so forth, would remarkably improve the performances of the life sensitive operations, in regard to safety, the agility of decisions and the ensuing actions.

## 5.4 Message Routing

Communication among different nodes in a wireless network raises problems that are not handled by standard distributed communication frameworks. For example, directed messages may miss a recipient because the recipient has moved. Therefore, there should be methods to support mobile communications. These would assist mobile agents to make their best effort for delivering messages and information to its destination. In a dynamic environment, it is critical for the local users and C2 decision maker to have access to the vital information in a timely fashion. To tackle this issue there are numbers of algorithms designed to establish a reliable communication for the message delivery throughout the networks.

On method that is proposed by Gray (2000) is the APRL algorithm. APRL is initially designed by Karp (1998) at Harvard University. APRL is an algorithm applicable in the communication networks and it could provide the basic routing functionality in a given dynamic network. According to APRL algorithm, each node of the network continually broadcast "ping" packets. A receiver that receives a "ping" packet knows that it is in transmission range of the sender and marks the sender as an immediate neighbour. The ping packet includes the complete routing table of the sender (Li and Rus, 2000), and the receiving node also adds routes for those other nodes that are reachable via the sending device. As the devices and nodes move relative to each other, they receive ping packets form different sets of neighbour devices and then update their routing tables accordingly.

According to Gray (2000) the most important advantage of the APRL algorithm is its simplicity, but on the other hand it generates more control traffic than desired and in some situations particularly when the network bandwidth is a scared resource this traffic poses as obstacle to network performance (McCabe 2003).

Another routing algorithm proposed by Karp (2000) is GPSR. Under the GPSR algorithm, the sending node (device) searches for the physical location of the target device, and then sends the message to the neighbouring node that physically is closest to the target's location. Due to variation in nodes distribution, there might be times when there is no neighbour closer to the target. To handle this, GPSR sends out probe packets to map the boundaries of the regions that contain no network node. As the result packets are routed around the edge of these "invalid" regions when necessary. In GPSR algorithm, packets mostly try to travel in the regions that there is the less possibility of lost and being wasted. This would increase the efficiency of the packets in terms of meeting their targets. According to Gray (2000) GPSR generates less control traffic than APRL, but does require a robust lookup service.

The routing algorithms above identify a rout between two nodes, but of course only if a rout physically exist (Gray, 2000). In a dynamic wireless network, there might never be a moment at which there exists a complete rout from the source to the target device. Instead the message must be sent partway through the network, and then sent the rest of the way once the changing connectivity opens up a path to the target. In other words, as Gray (2000) describes there must be another layer on top of the basic routing system to handle network disconnections. The goal of this layer is to queue messages as "close" as possible to the critical disconnection, so that the data can be forwarded as soon as the disconnection goes away.

There are several approaches to constructing this layer, but one of the most promising one is “active messaging” method (Okino, 1999). Active message just not follows a fixed algorithm instead each message specifies its own routing strategy, possibly in form of procedural code that is attached to the message. The advantage of active message is that each application can apply an application specific routing policy to its own message (Gray, 2000). There could be different strategies adopted or designed for different applications. For example, one application might use a routing strategy that replicates high priority message at key network points and then sends the copies along different paths. Others might use simple strategies such as one proposed by Gray (2000) that each message is sent to whichever reachable machine most recently had a connection to the ultimate target. The message waits on that machine until the target is once again reachable.

It is worth mentioning that in this routing method the key challenge is to identify the most appropriate routing and active-messaging strategies (Gray, 2000).

Mobile agents also show the considerable potential in order to couple with active messaging method in a dynamic wireless network. Mobile agents are autonomous and adaptive and they can be used to move computation to more attractive network locations and often to avoid the use of unreliable or low bandwidth network links. As Gray (2000) explains the active messaging system can be implemented on the top of the mobile-agent system. Each message and routing strategies is wrapped inside a mobile agent, which carries the message through the network. Although a production system would be routed much closer to the network layer, but implementing the system on top of the mobile agent system allowed extremely rapid development and more flexible routing strategy adoption.

## 5.5 Mesh Networks

As the literature on public safety shows (eg Corson and Macker, 1996; Commtech Agile Project, 2003; Smith and Tolman, 2000; Poor, 2003) there are three major communication issues facing responders at a typical incident.

1- Reliability and scalability of communications
2- The ability of tracking and locating personnel and assets throughout the operation field
3- Interoperability with other agencies

In fact in a real combat or emergency first response operation, communications may be facilitated through rapidly-deployable cellular infrastructures. However, in frontline areas, or during multi-task operations or rapid changing environment, conditions are often chaotic. Highly mobile units, such as vehicles, quickly detach from their groups to join and support others teams or individuals. Within these groups, the networking technology supports their communications must be instantly reconfigurable, yet completely decentralized, redundant and survivable, in short, a mobile wireless make-up (Corson and Macker, 1996).

As Poor (2003) describes there are different types of network topologies that might be considered to support these requirements. One network topology is the point-to-point networking configuration that can provide reliability of the communication, but it doesn’t scale to handle more than one pair of end points especially in a mobile setting. Another potential topology is point-to-multipoint networking. This technology can handle more end points, but yet the communication reliability is determined by the placement of the access point and end points. Also it has capacity is limited and it just can support number of the mobile users who move in its wireless range. So, if environmental conditions result in poor reliability, it is difficult or even impossible to adapt a point-to-multipoint network to increase reliability.

Therefore, there should be a network topology that could address these issues in order to support reliable and efficient operation in the public safety environment.

Mesh networks addresses these issues with advanced peer-to-peer and position location capabilities. The wireless mesh network topology is a point-to-point-to-point, or peer-to-peer, system called an ad hoc, multi-hop network (Poor, 2003).

According Feldman(1998) from to RAND Corp., mobile mesh networks were an outgrowth of the earlier packet radio network concept. In such a network the goal is to provide robust point-to-point communications and information is divided into packets which are then delivered in a store-and-forward fashion via one or multiple hops. In such a network, packets associated with a given message can take different routes through the network. For messages that must be delivered quickly and also with high reliability, the associated packets might possibly be duplicated, with different copies following different routes through the network.

So, in a mesh configuration every node can send and receive messages, and also functions as a router to relay messages to its neighbours (Figure 5.1). Through the relaying process, a packet of wireless data will find its way to its destination, passing through intermediate nodes with reliable communication links.

Through the peer-to-peer router-based networks, a mesh network offers multiple redundant communications paths throughout the network. If one link fails for any reason then the network automatically routes messages through alternate paths.

In a mesh network, it is also possible to shorten the distance between nodes, which dramatically increases the link quality. Considering that the battery power consumption is a considerable issue in a wireless and dynamic environment, this characteristic of mesh network make links more reliable without increasing transmitter power in individual nodes. Another feature of the mesh network is the ability of extending the reach, adding redundancy, and improving the general reliability of the network simply by adding more nodes to the network.

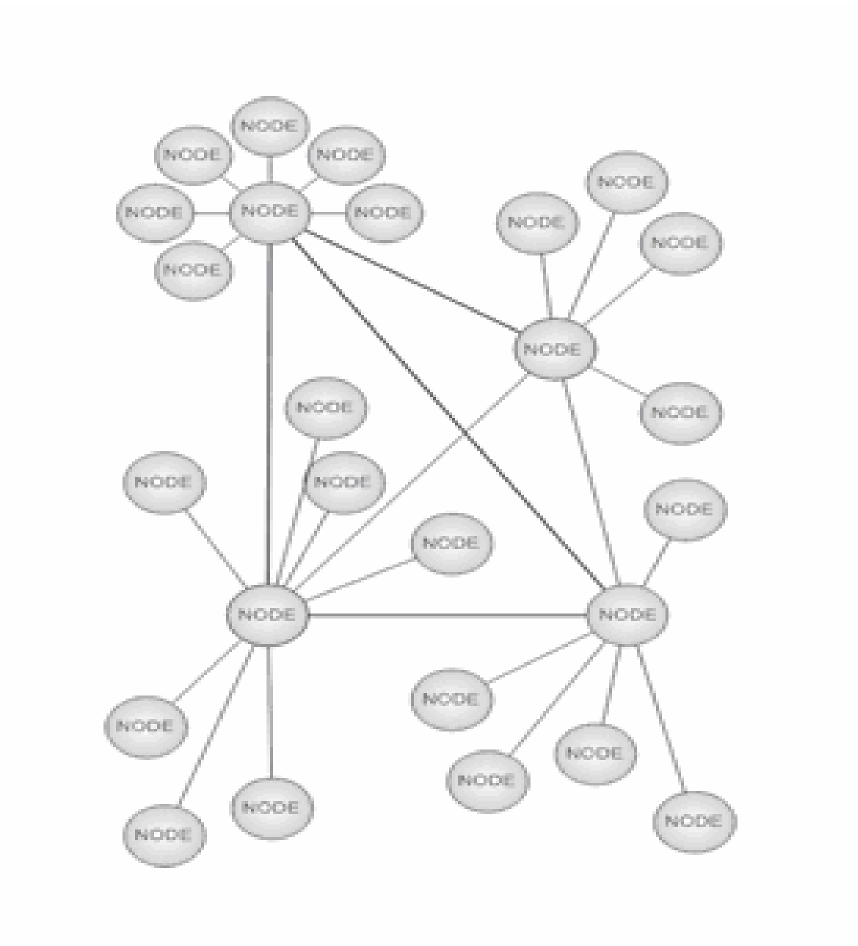


**Figure 5.1** A mesh configuration that every node can function as a router

As Poor (2003) spells out, the most promising characteristics of the mesh networks are:

- Self-Configuring and Self-Healing
- Inherently reliable and highly adaptable
- Redundancy and Scalability

The comparison among different wireless topologies made by Poor (2003) shows (Table 5.1) that how mesh network could fit properly to the public safety requirements.

| Comparison Table | | | |
|---|---|---|---|
| Suitability of different network topologies in public safety applications | | | |
| Topology | Reliability | Adaptability | Scalability |
| Point-to-Point | High | Low | None (two end points) |
| Point-to-Multipoint | Low | Low | Moderate (7-30 end points) |
| Mesh Networks | High | High | Yes (thousands of end points) |

**Table 5.1** Comparison of different wireless topologies (Poor & Hodges, 2002)

Despite all of the promising benefits of the mesh networking in a dynamic environment, there are serious problems regarding the technical features of this topology. As Feldman (1998) form RAND Corp., expresses, the obvious drawback of the mobile mesh architecture is the extra complexity at every node for keeping track of network states, routing information and packets buffering. In fact mobile mesh networks will have to be more costly than hierarchical (non-self-organizing) networks with mobile backbones because all nodes in a peer-to-peer network must be able to buffer multiple packet streams, route packets, and store information about the state of the network. However, many of these problems as discussed earlier can be handled by using mobile agents as an entity with autonomy throughout the network.

In order to clarify how mesh networks can be applied in the public safety operations, the following section will provide two scenarios to show how the mesh networking could be applicable in this area. The first scenario is a fire scenario that might happen in the urban areas and the second scenario is a situation that law and enforcement forces aims to protect the civilians against an imminent chemical threat. In both scenarios mesh networking is being applied to establish the reliable communications between different levels of users in order to support the situational awareness for the users in the front line and decision makers.

### 5.5.1 Scenario 1 (Civilian fire event)

Consider a situation where a fire has broken out in a mid-rise building. Mesh networks can improve first responders' efficiency and safety, while dealing with this incident.

In such a scenario, first responders can take advantages of the mesh networks capabilities in many ways. As a primary application, vital information about the incident, such as maps and blueprints, the presence of hazardous materials, occupancy or other pertinent facts, can be sent to fire and rescue teams en route, since mesh networks support broadband wireless communications to vehicles moving heading to incident location. In this situation, the wireless mesh enabled vehicles can also act as hopping points, extending communications links to other vehicles and authorized users moving in their range. Also on the scene, mesh networks enables an ad hoc high capacity network to instantly form at incidents even if the primary network has been damaged around the incident, or the incident site is out of range of the primary communication systems (Figure 5.2).

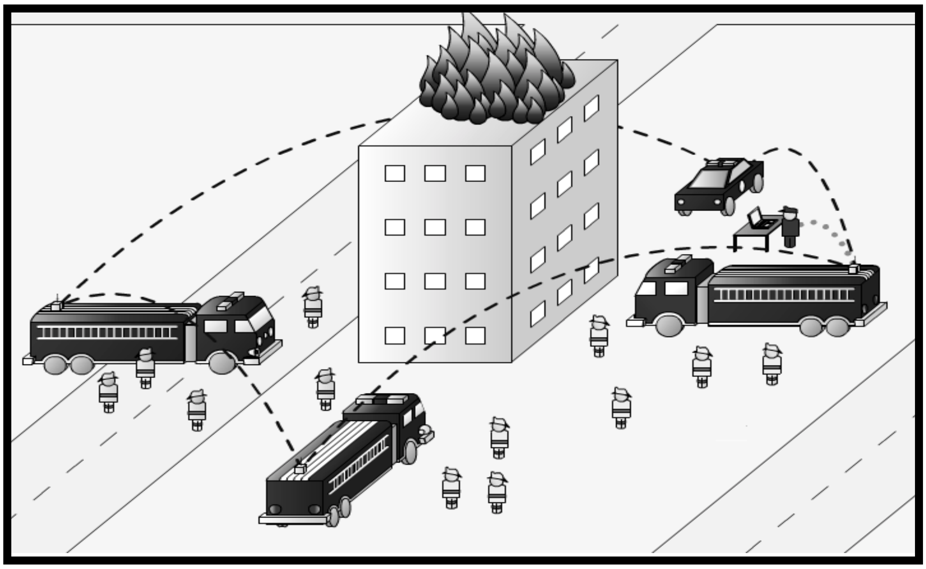

**Figure 5.2** An ad hoc wireless network supported by mesh topology at the scene (Motorola, 2004)

In this configuration, the multiple peer-to-peer networked communication groups can be formed, based on the needs of the applications being used, or as determined by the incident commanders. This is fairly compatible with the SUO model and shows the advantages of this model in this situation. This means that mesh networking could support properly the SUO model communications properly (Figure 5.3).

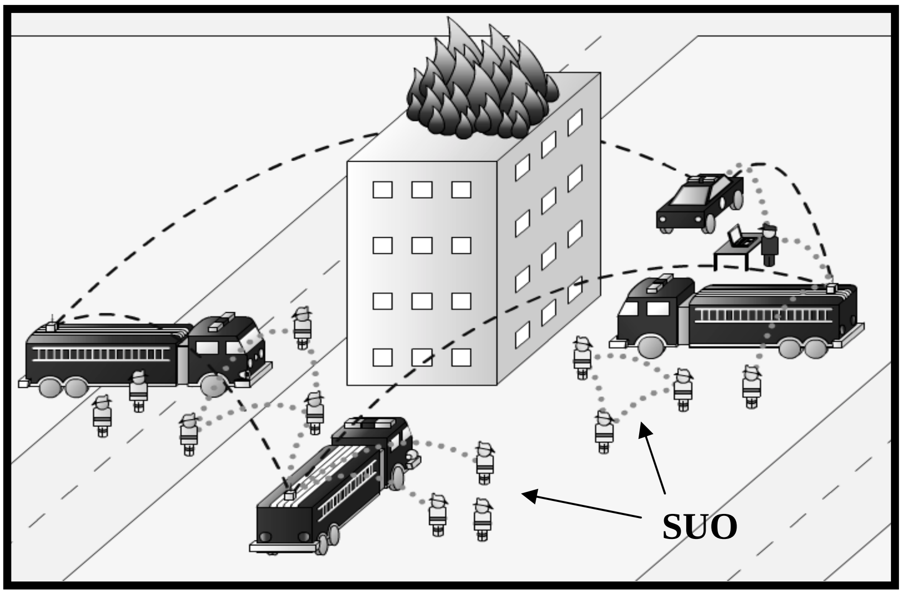


**Figure 5.3** Compatibility of mesh networks and SUO (Motorola, 2004)

At the operational scene, one of communications of particular concern is communications to and from first responders inside a building. Also communications can be a problem if the building structure is not conductive to radio propagation, or when radio transmissions must penetrate multiple floors (Motorola, 2004).

In this situation using the mesh network technology would help to cope with the low bandwidth problem. As researchers in the Motorola Corporation (2004) describe, in such a scenario, instead of trying to blast sufficient bandwidth through an environment using bulky, high-power, amplified radios, it is possible to use a mesh network enabled incident communications system which leverages mesh networks' multi-hopping technology, via small, battery consuming wireless routers. As part of the system, these devices can be pre-deployed, or placed as first responders move through the building to provide connectivity. In fact, the mesh-enabled routers provide a pathway for communications into and out of the building. They also enhance communications between groups inside the building (Figure 5.3). Research by Motorola Corporation (2004) also reveals that telemetry, video, or backup voice communications can be sent through this mesh network architecture.

Moreover, the mesh network enables the tracking and location of first responders inside buildings. Portable routers can be deployed in and around the building to supplement vehicle mounted wireless routers in order to accurately determine the location of the first responder inside buildings (Figure 5.4).

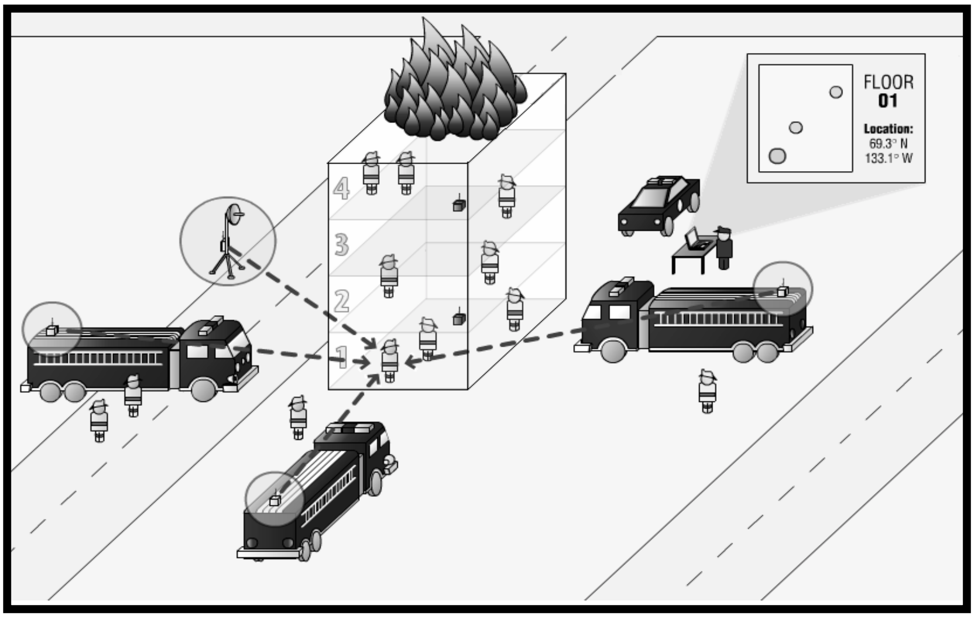


**Figure 5.4** determining the location of the first responder inside the buildings (Motorola, 2004)

Working together, these devices can track and locate mesh-enabled devices in most structure. This increases safety and reduces the voice chatter required for position reporting (Couper, 2004).

Also the industry standard IP protocols, utilised by many off-the-shelf applications and devices, are transparently supported by the mesh networks (Couper, 2004), simplifying interoperability with other agencies (Figure 5.5) .

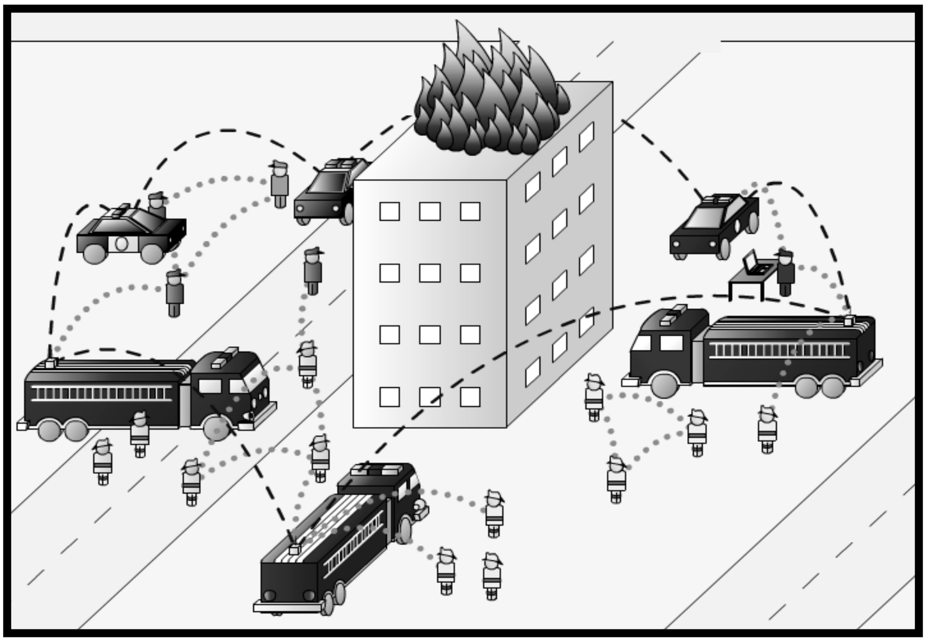

**Figure 5.5** Different public safety agencies can communicate to each other (Motorola, 2004)

In mesh topology, networks are inherently scalable (Poor, 2003). Peer-to-peer networking technology enables efficient use of the available spectrum. Incident communications can be segmented onto different groups and some, or all, of these groups can be connected together.

If the incident falls within the coverage area of the wide area mesh network, voice, video and data can be wirelessly sent to and from remote, command or operations centres. This would help the decision makers in the C2 to make more effective decision based upon the more reliable information they receive and pass their orders to the related teams more quickly.

In summary, this scenario shows how mesh networks can significantly increase the situation awareness of the first responders crew and provide them with more agile and safer operation environment.

### 5.5.2 Scenario 2 ( Dangerous area isolation)

In this scenario a situation is considered where the law enforcement would use mesh network technology in order to isolate a dangerous area and protect the civilians against any likely threat. In this scenario, the incident is a hazardous waste spill in a busy section of town (Figure 5.6).

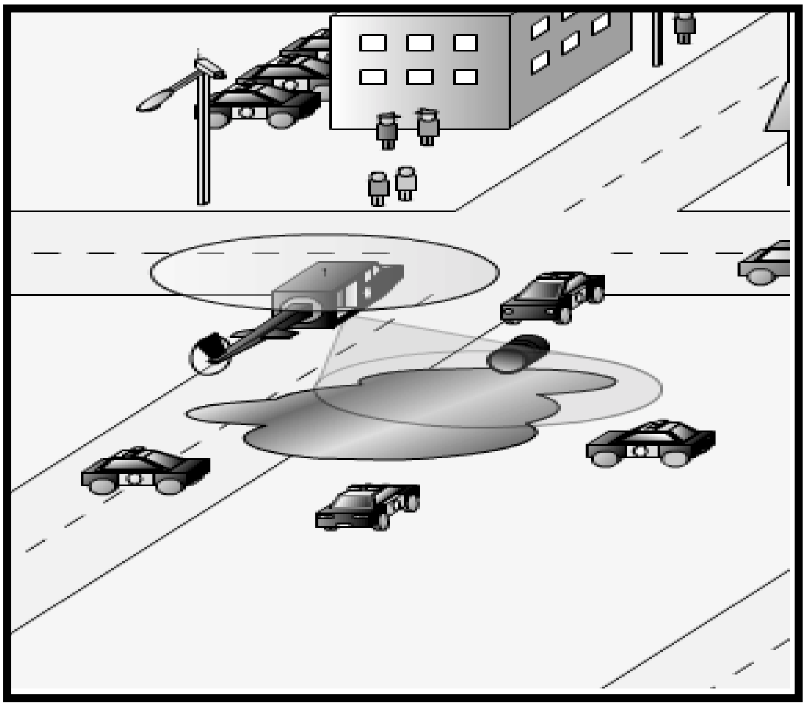

**Figure 5.6** Isolation of dangerous area to protect civilians (Motorola, 2004)

In this scenario, mesh networks enable several high-speed networks to form instantly at an incident site, sharing and exchanging critical information among each other (Motorola, 2004). For example, by the use of mesh networks, video from the helicopter is sent to the officers on the ground to increase their situational awareness. Also high bandwidth networking is supported by the mesh topology even if an incident occurs out of range the main network. This would make it easier for the additional units to be instantly and automatically added to the local network and users can hop onto the main network at any time, if they are within range (Figure 5.7).

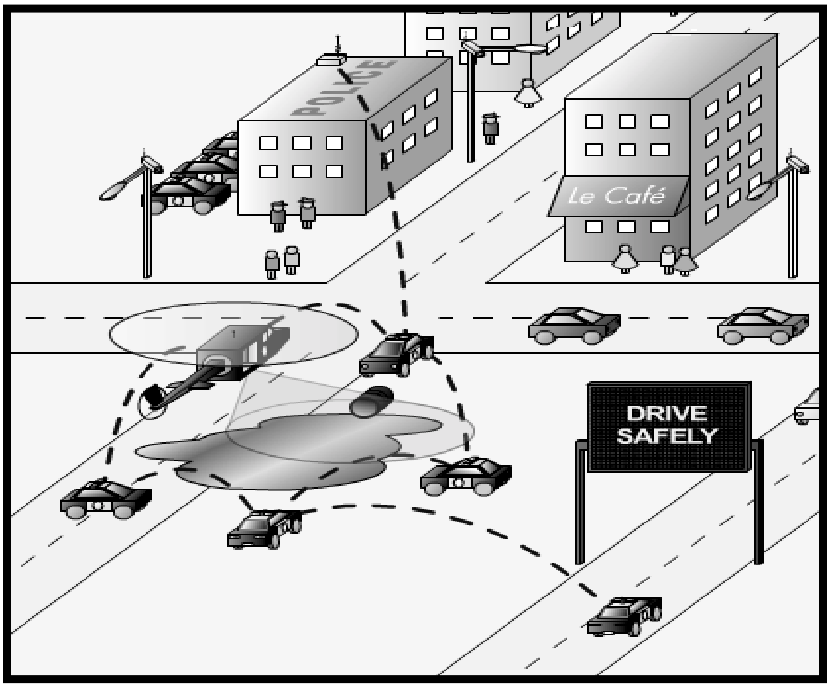


**Figure 5.7** Set up a fast and reliable network instantly at the scene (Motorola, 2004)

Furthermore, mesh enabled users and devices can leverage and interoperate with other agencies, including those deployed to support emergency response.

The significant outcome of this scenario is the way that mesh network can help better and reliable information sharing in a team which leads them to a better cooperation and safety.

Both of these scenarios strongly show that mesh networking topology is the best option among other available topologies since it fairly fits to the public safety requirements and their operating environment.

## 5.6 Ultra Wideband technology

As discussed above, mesh networking is a promising topology to work in dynamic, infrastructure situations such as public safety environment. The next issue is to find out which wireless protocol and radio communication can fit properly to this topology.

Ultra Wideband is an innovative wireless technology that can transmit digital data over a wide frequency spectrum with very low power and at very high data rates.

As well as having the ability to transfer high-speed data using low power, Ultra Wideband can carry signals through many obstacles that usually reflect signals at more limited bandwidths and at higher power.

According to researches carried out at Roke Manor Research institute (2004) Ultra Wideband communications can provide short-range links at a high rate of data i.e. around 110 Mbps. They operate across a large range of frequency bands, with only negligible interference to existing systems using the same spectrum. This is achieved by spreading the transmit power over a broad range of spectrum from, say, 3.1GHz to 10.6GHz giving a lower power spectrum density figure.

UWB is simple in principle. In UWB, very short pulses, which carry data, are sent from the transmitter to the receiver and the narrow pulse leads to the wide spectrum. This in turn allows a low power spectral density for a given transmission rate, leading to the claim that it will not interfere with other users of that band. The pulse rate will be determined by a number of factors. In many applications each may carry one bit of data. Even for a data rate as high as 500 Mb/s a transmitter will still only have a low duty cycle (Hulter and Streeton, 2003). This therefore gives the potential for many transmitters to operate at the same time in the same area with acceptable interferences. UWB devices can perform a number of useful telecommunication functions that make them very appealing for the public safety.

DARPA has conducted a Networking in Extreme Environments (NETEX) program in order to investigate the application of UWB in the extreme environments such as military and public safety operations environment. According to Miller (2003) from the NETEX research group, the goal of the NETEX program is the development of "robust and rapid wireless networking in complex, hostile environments using UWB technology." The meanings of the several descriptive words in this statement of the project goal were given as follows:

• *Robust* means a networking scheme and implementation that has immunity to channel fading and equipment outages.

• *Complex* means an operational environment that is relatively harsh to radio communi-cations and/or is subject to the scenario- and location-dependent propagation properties, such as dense urban, indoor, and aboard-ship situations.

• *Hostile* means an environment that necessitates operation with low probability of detection to avoid jamming.

• *Rapid* means networking that can be configured "on the fly" as *ad hoc* networks and without reserving or contending for a spectrum assignment.

• *Using UWB technology* indicates that the attributes of the operational scenario are such that UWB technology is considered to have a particular advantage in meeting the communication system performance requirements.

Results from the NETEX research shows that these systems have very wide information bandwidths, are capable of accurately locating nearby objects, and can use processing technology with UWB pulses to "see through objects" and communicate using multiple propagation paths.

Other research groups and researchers (Intel. 2004, Motorola. 2003, Roke Manor Research 2004, and Fontana 2004) have investigated the properties of UWB and the benefits of using this technology over other wireless protocols. The advantages claimed for UWB technology is providing reliable and adequate communications in the extreme environment. The results of this research are summarized in following table (Table 5.2).

| UWB Property | Advantages |
|---|---|
| Very wide fractional and absolute RF bandwidth | • High rate communications<br>• Potential for processing gain<br>• Low frequencies penetrate walls, ground<br>• Frequency and bandwidth adaptive |
| Very short pulses | • Direct resolvability of discrete multipath components<br>• Diversity gain<br>• Extremely difficult to detect |
| Persistence of multipath reflections | • Low fade margins<br>• Low power<br>• High multipath immunity |
| Carrier-less transmission | • Hardware simplicity<br>• Small hardware |
| High-speed throughput | • Fast, high-quality transfers |
| Low power consumption | • Long battery life of portable devices |
| Silicon-based and standards-based radios | • Low cost nearly "all digital" architectures |

| | |
|---|---|
| Wired connectivity options | • Convenience and flexibility |
| Low transmit power | • It transmits negligible interference to existing system<br>• Systems to operate across a range of frequency bands unlicensed |

**Table 5.2** Pproperties of the UWB and its benefits

As discussed above, UWB has features and advantages that make it appealing for applications used in extreme environments. Emergency events involving critical issues of public safety is one important area that could take advantage of the UWB technology for the communication purposes since such event occur in what is is known as an extreme environment with specific communication requirements. Many of these requirements could be properly addressed by the UWB features for example high data rate, high multi-path immunity, fast and high-quality data transfers, low power consumption, low frequencies penetrate walls and ground and, so forth.

Another important characteristic of the UWB is its ability to fit properly in a mesh network configuration. This is vital to the public safety to use a wireless radio technology that could support and fit to the recommended mesh network topology. In general, UWB shows many advantages over the other popular wireless technologies (Table 5.3) such as IEEE 802.11a, IEEE 802.11b (Wi-Fi), IEEE 802.11g, Bluetooth and, Zigbee (Motorola Inc. 2003, ZigBee Alliance 2004)

| Specification / Technology | Data Rate | Multimedia Support | Power Consumption | Mesh Support |
|---|---|---|---|---|
| IEEE 802.11a | 54 Mbps (actual payload rate of 35 Mbps) | No, due to protocol inefficiencies and overhead | High 1.5 to 2W | No. P-M |
| IEEE 802.11b(Wi-Fi) | 11 Mbps | No, due to protocol inefficiencies and overhead | High 1 to 2.2 W | No. P-M |
| IEEE 802.11g | 11 - 54 Mbps (actual payload rate of 35 Mbps) | No, due to protocol inefficiencies and overhead | High 1.5 to 2.5W | No. P-M |
| Bluetooth | Less than 1Mbps | No, due to low data rate connections | Moderate | No. P-P |
| Zigbee | 250kpbs | No, due to low data rate connections | Low | Yes. P-P-P |
| Ultra Wideband | ~ 250 Mbps | Yes | Low | Yes. P-P-P |

P-M: Point to Multipoint, P-P: Point to Point, P-P-P: Peer to Peer to Peer

**Table 5.3** Comparison between different wireless standards

A careful look at the current wireless solutions reveals that the problematic trade-offs between data rate, power consumption and mesh networking is evident. These trade-offs are less a problem when UWB is being used as the wireless solution for the communication purposes. This attribute of UWB make it again very interesting for the public safety operations since it decrease the problems of having low power consumption, high data rate and mesh networking at the same time.

The following scenario clarifies the case for UWB: Imagine a situation where a network node (A) wishes to communicate with node (B), which is, say 30m away (Figure 5.8). Using UWB wireless technology the available bandwidth directly between the two nodes is 100Mbs. However, located halfway between node (A) and

(B) is node (C), 15m from each. The available bandwidth to nod (C), because of the shorter distance is 200Mbs from each node. Using node (C) as a relay and assuming that node (C) can handle the traffic, (A) and (B) can communicate at 200Mbs, over twice as fast as via the direct path. Thus one advantage of using mesh topology along with the UWB is that throughput is increased.

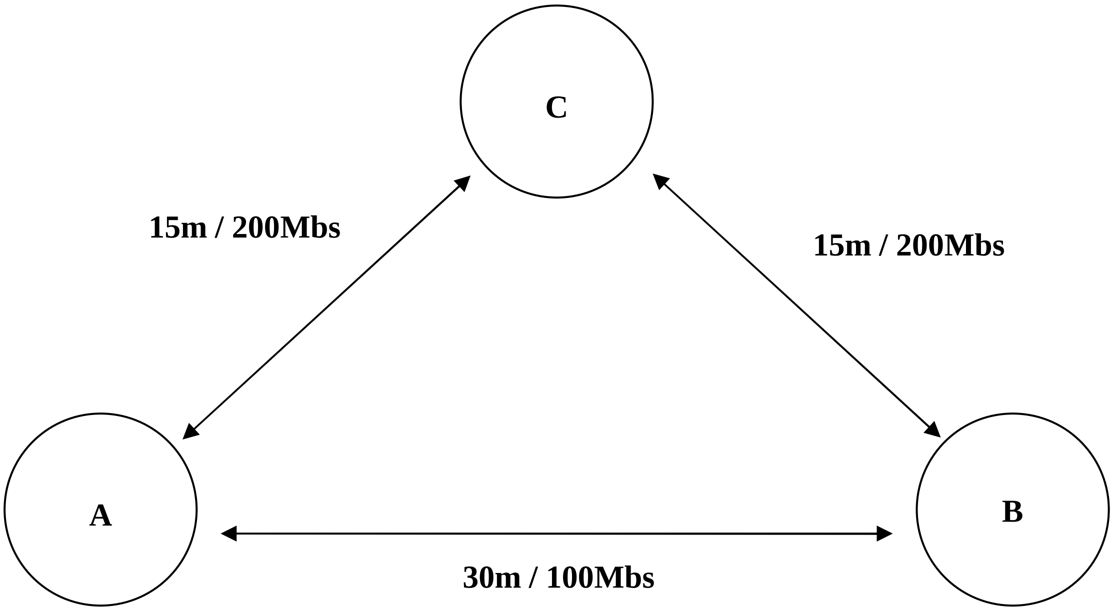


**Figure 5.8** Communications scenario through UWB

A consideration of the above scenario shows that another advantage of UWB is its ability to support the long distance communications even in impossible places can only be reached with the same bandwidth. It these situations, nodes far from each other, which would not be normally be in radio range of each other, can communicate via intermediaries in a high bandwidth fashion.

Considering that mesh networks can get round obstacles by using strategically placed repeaters; for example, through thick or metal lined wall, or up an escalator in a subway station, their combination with the UWB wireless technology allows a very effective installation of a communications infrastructure for cluttered environments. Scattering repeater modules to shape a mesh network will allow transmitting bandwidth hungry information to every node of the network.

In fact, the best topology that would support the UWB efficiently is the mesh topology. As a characteristic, UWB wireless bandwidth drops rapidly as distance increase (Artimi, 2003). This property of the UWB is a fundamental property since the signal power is limited at the transmitter and also at the receiver by the thermal or electromagnetic noises in the receiver and amplifiers.

On the other hand, UWB can support tens and, depending on the implementation, potentially hundreds of simultaneous non-interfering channels, within radio distance of each other. In this sense, using a mesh allows the network to trade some channels for increased performance since the mesh architecture creates more capacity and more coverage as more users are enabled throughout the coverage area. In addition, ultra-wideband as the wireless transmission technology used in mesh topology allows very low cost and low power access points and high bandwidth within the coverage area. These are the power consumption and data rate requirements of emergency public safety situations that the other existing wireless solutions simply cannot meet.

## 5.7 Sensor Networks

As mentioned in previous sections, communication systems play an essential role in emergency situations. However, existing communication systems in the public safety often provide minimal communication infrastructure for supplying information about the nature a disaster and its extent. As a result, first responders typically enter emergency scenes with little real-time information about the site, and only a chaotic means of rescue are available to them to protect them trapping in the unpredictable situations. According to Ray et al.. (2003) one promising method for providing real-time feedback from disaster sites involves the use of sensor networks.

Sensor networks are heavily relying on sensors as the interface with the environment and wireless technologies that handle the data flow. As Karl and Willig (2003) describe, these networks combine simple wireless communication, minimal computation facilities, and some sort of sensing of the physical environment into a new form of network that can be deeply embedded in the physical environment. Typical sensing tasks for such a network could be temperature, light, vibration, sound, radiation, etc (Lewis, 2004). In a sensor network each sensor node is comprised of radio front end, microcontroller, power supply and the actual sensor (Karl & Willig 2003).

In reference to the requirement of the public safety tasks, Ray et al. (2003) spell out that many essential tasks of an emergency response system require the following capabilities:

• To enable team members to identify their own and others' locations.
• To locate victims, potential hazards, or sources of the emergency.
• To identify and rescue trapped personnel.

Research carried out by Ray et al. (2003) shows that none of the previously proposed systems have been designed for the specific working conditions of emergency networks, and they are generally unsuitable for this purpose. As Ray et al. (2003)

explain the main reason of this issue is that these systems can not respond properly to the emergency first responders' needs, is the lack of their robustness against equipment failures and changing structural topology.

On the other hand, Lewis (2004) mentions the requirements for emergency responders and explains that, in order to cope with situations in an extreme environment; having distributed networks of sensors that can be deployed easily, be installed fast and have self-organizing capabilities is a promising solution. Following this argument, Lewis (2004) describes that how wireless sensor networks satisfy these requirements.

According to Lorincz et al. (2004) sensor networks are new class of devices and have the potential to revolutionize the capture, processing, and communication of critical data for use by first responders. They believe that sensor networks represent the next step in wireless communication's miniaturisation, and their power and size make it feasible to embed them into wearable vital sign monitors, location-tracking tags in buildings, and first responder uniform gear.

Sensor networks show unique characteristics that make them appealing for critical public safety applications. According to Karl and Willig (2003) these networks share many commonalities with existing ad hoc network concepts which is one advantage these networks have with the technologies for ad hoc networks. However Karl and Willig (2003) indicate that some of the most important similarities and differences of the wireless sensor networks (WSNs) as follow:

1- *Application specificity*: Due to the large number of conceivable combinations of sensing, computing and communication technology, many different application scenarios become possible.

2- *Environment interaction*: Since these networks have to interact with the environment, their traffic characteristics can be expected to be very different from other, human-driven forms of networks. A typical consequence is that WSNs are likely to exhibit very low data rates over a large time scale, but can have heavy bursting traffic when something happens.

3- *Scale*: Potentially, such WSNs have to scale to much larger numbers (thousands, hundreds of thousands) of entities than current ad hoc networks, requiring different, more scalable solutions.

4- *Energy*: Similar to some forms of ad hoc networks, energy supply is scarce and hence energy consumption is a primary metric to be considered.

5- *Self configurability*: Similar to ad hoc networks, WSNs will most likely be required to self-configure into connected networks, but the difference in traffic, energy trade-offs etc. need to be considered.

6- *Simplicity*: Since sensor nodes are small and energy is scarce, the operating and networking software must be kept simpler as compared to current desktop computers.

Characteristics such as scale, self configuring, energy consumption and simplicity, implies that sensor networks should fit to a type of network topology that can support WSNs' characteristics. Among the different network topologies, mesh networking seems to have more promises and compatibility in supporting the WSNs. Albowicz et al. (2001) describes that although a single sensor node cannot replace a properly equipped human observer, the scale, persistence, and low cost of a mesh of many such nodes provides a better solution for a large variety of situations.

Lewis (2004) holds the same opinion on the sensor networks and states that mesh networks can be good models for large-scale networks of wireless sensors that are distributed over a geographic region. According to Albowicz et al. (2001) rapid, ad hoc distribution and auto-configuration of a WSN can be achieved with a decentralized network solution like a mesh topology. They argue that a centralized solution often involves prohibitive overhead for delivering input to a “server” and processing collected data, as well as the difficulties of disseminating that data back to the sensors or providing unique mappings for a massive and unreliable sensor array.

Although wireless sensor networks compatibility with the mesh topology is shown to be a promising communication system for the emergency first responders and public safety tasks in many areas, there is still much development work to be done and WSN faces considerable challenges before its wide-scale adoption.

According to Lorincz et al. (2004) in a WSN sensor nodes' extreme resource limitations represent remarkable challenges in protocol design, application development, and security models. Also Karl & Willig (2003) spell out that there are serious problems regarding the sensors size and costs since the technology needs to be more mature and advanced. However the possibilities exist that sensor networks could potentially become an extremely useful technology for these type of applications when the basic size and cost problems are solved. Studying these challenges and the corresponding solutions could be the subjects of the future research.

## 5.8 Agent Framework

The case study described in Chapter 4 of this thesis shows that problems confronting the human decision-makers are rapidly increased in critical emergency situations due to complicated tasks in uncertain environments, with a short time-frame for making decisions. In natural and man-made disasters, such as environmental cleanup operations, or civilian and military crisis responses, different organizations such as fire fighters, police, and medical assistance personnel need to cooperate in order to save lives, protect structural infrastructure and property, and evacuate victims to safety.

In such environments, human rescuers must make quick decisions under stress, and get victims to safety, often at their own risk. In order to achieve this goal they must have timely and accurate information on the status of the environment and also must coordinate the allocation of resources and other rescue activities.

These problems considerably affect team performance since the actions and performance of team members are strongly tied with their decisions. To be successful, team members must understand how to gather, summarize, interpret, and use information to perform their tasks. MURI (1998) research project shows that characteristics distinguishing successful teams from unsuccessful ones include team self-awareness, within-team interdependence, performance monitoring, feedback, clearly communicating intentions, and helping teammates when needed. Also Lexon et al. (2000) believe that team members must understand their role in the task, what information is required by their teammates and be aware of and act in accordance with the strengths and weaknesses of them. In fact tasks confronted by teams often require individual specializations, separated locations, and differing responsibilities (Sycara et al., 2003).

Acoording to Lexon et al. (2000) in recent years, the approach used to solve complex problems in organisational teams has shifted from developing large, integrated legacy software systems, to that of developing small, autonomous, intelligent software components that can interact with humans, with other software components, and different data sources. These *agents* may provide specialized or periodic information from certain information sources, or may perform some task or service based on the information they are given.

In the other word, to aid teamswith common objectives in fast changing, multi user environments, agents must develop greater capacities for modelling users and situations, preparing and communicating task information, adapting to changes in situation and capabilities of other team members.

To achieve these aims, Lexon et al. (2000) research shows that software agents can be deployed in support of team performance in different ways, including:

- Support the individual team members in completion of their own tasks;
- Allocate to the agent its own subtask based on the new changes;
- Support the team as a whole

In addition, Sycara et al. (2003) state that agent assistance will be particularly critical to dynamic environment tasks such as military and emergency operations. In such an environment, operations of teams become more agile and situation specific since a primary mechanism for coordination will be their networked information systems and the information travel through it. Sycara et al. (2003) argue that in this uncertain environment supporting teamwork is crucial and software agents are well suited for this task because the domain independence of teamwork agents would allow them to be rapidly deployed across a broad range of tasks.

However they believe that the greatest hurdle to providing human users with assistance by agents, rests in the communication with the user who engaged to an agent and making the agent’s results understandable to the human. So, for software agents to work effectively they should be implemented and perform within a functional system.

This is the point Sycara et al. (2003) describe by stressing that no single agent could provide all the forms of assistance for diverse members of a team. They believe that a system comprised of multiple, functionally specific agents, can configure itself as needed to deliver the right support to the team and its members. This system should be tailored to the team's particular task and situation.

Sycara et al. (2003) propose a general framework for a multiple agent system called RETSINA (Reusable Environment for Task Structured Intelligent Network Agents). Figure 5.9 shows a re-usable multiagent infrastructure which provides a domain independent, componentized framework to allow effective human-agent interaction.

RETSINA provides facilities for reuse and combination of different existing infrastructure components and also defines and implements an individual agent architecture that provides higher level agent services, such as planning and execution of various tasks. RETSIAN provides a multiagent infrastructure for finding, assembling, and coordinating teams of agents to accomplish specified goals. According to Sycara et al. (2003) RETSINA agents can support human teams by supporting the task of individual team members and also act as team members or support the team as a whole.

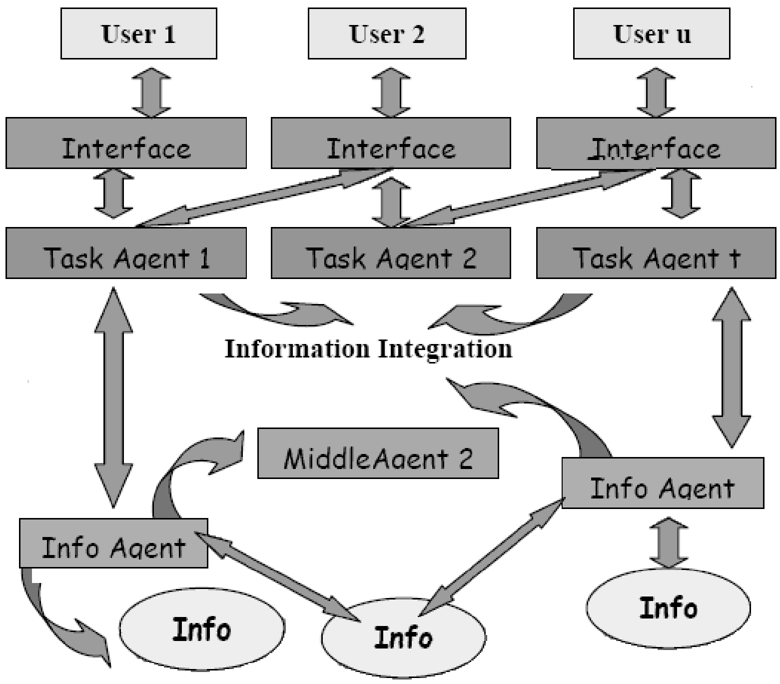


**Figure 5.9** RETSINA framework (Sycara et al.., 2003)

The significance of RETSINA is the generality of its framework that can be used to develop other systems and framework for supporting teamwork. One important application of this general and re-usable framework is the area of disaster response (Nourbakhsh et al.., 2005; Schurr, 2003). For example Nourbakhsh et al. (2005) propose a framework for disaster team management. In their disaster response team instantiation, they used RETSINA to categorize agents into the following four types based on their function. *Interface agents* facilitate user interaction. *Task agents* seek to accomplish user goals. *Middle agents* provide infrastructure for dynamic runtime discovery of agents that can perform a given task. *Information agents* can access various external information sources, such as disaster site blueprints, hazardous materials shipping records, and other vital information.

Lexon et al. (2000) propose a reduced framework to assist teams tasks within a changing environment, again based on the RETSIAN. In their framework there are three classes of agents, namely: *interface agents, task agents,* and *information agent*. *Interface agents* interact with the user, providing a mechanism whereby humans can specify tasks and inspect the results. They may acquire, model, and utilize user preferences to guide system coordination in support of the user's tasks. *Task agents* help humans perform tasks by formulating problem solving plans, and carrying out these plans through querying and exchanging information with other software agents. *Information agents* provide intelligent access to a heterogeneous collection of information sources.

These frameworks the choice of framework proposed in this study ( Figure 5.10) of mobile agents based on RETSINA. In this framework there are three types (class) of agents: *Interface agent, Mobile agent, and Information agent. Interface agents* make possible user interaction and provide a method by which individuals are able to identify their tasks and check the results. *Mobile agents* can move throughout the network and establish the communication among other agents and entities. In fact they are middle agents that which provide infrastructure for dynamic discovery of agents that can perform a given task. The can also seek to accomplish user goals and help humans perform tasks by planning the tasks and exchanging information with other software agents. *Information agents* can access various external information sources and provide access to an external collection of information sources.

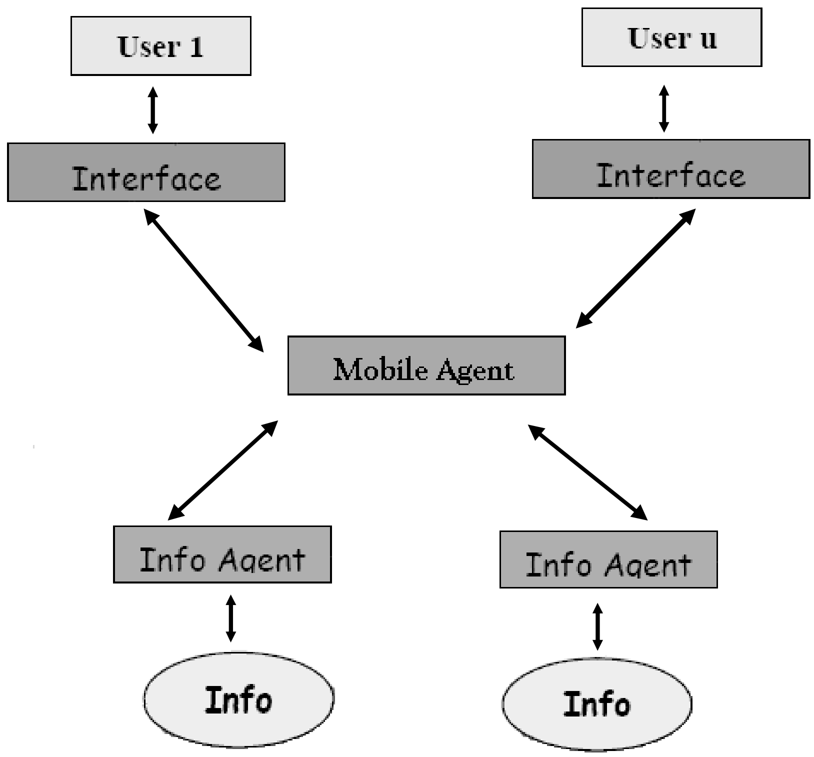


**Figure 5.10** Proposed framework based on the mobile agent (Derived from RETSINA)

Despite advances in agent technologies, human involvement in this framework will be crucial. According to Sycara et al. (2003) in almost all cases today the limiting factor in human-agent interaction is not about computing cycles or connectivity (the machine side) but the user's ability and/or willingness to communicate his desires and sift, organize, and interpret the machine's response to satisfy them (the human side). Allowing humans to make critical decisions within a team of intelligent agents is prerequisite for allowing such teams to be used in domains where they can cause physical, financial or psychological harm.

These critical decisions include not only the decisions that, for moral or political reasons, humans must be allowed to make, but also coordination decisions that humans are better at making due to access to important global knowledge, general information or support tools. For these reasons the next section of this chapter will discuss these issues to emphasize on the role of humans in decision making specially in time sensitive and critical situations.

## 5.9 Human, the ultimate decision maker and actor

Humans are the key players in the emergency first response tasks and there is a danger in believing that technological advances alone will provide solutions. Although they use different types of technologies to help them accomplish their tasks, these technologies cannot work without any meaningful context. These contexts are shaped through the social interactions of humans and the ways they use technologies within these relationships. As Kling’s (2000) research reveals, the ‘social context’ of information and communication technology development and usage play a significant role in influencing the ways that people use information and technology. According to Kling (2000), social context refers to a specific matrix of social relationship and it influences the consequences for work, organizations, and other social relationships. This means that it is crucial to study technologies in their relations to human activities, specially those technologies that significantly affect human’s activities when applied in the public safety operations.

Literature from the public safety domain (Agile Project 2003; Payne et al., 2000; Yufik, 2003) shows that emergency response tasks in both military situation and civilian operations are characterized by environmental uncertainty, high stress atmosphere, and time criticality of decision making. Normally in the emergency response operations, the decision making process is distributed across different team members with different expertise. These people are distributed in space and time and act with incomplete information within an uncertain environment.

Diverse technologies such as mobile agents and wireless technologies are designed in order to cope with such unpredictable environments, helping better decisions to be made. According to Payne et al. (2000), the agent metaphor is suitable for developing software technology that can act to interact with computer processes that assist human decision making. As discussed earlier, software agents can reduce the amount of interaction between humans and the computer system and allow the humans to concentrate on other activities, such as assessing the situation, making decisions, or reacting to changes in the system. Payne et al. (2000) argue that software agents also should bring more value for decision makers through active and intelligent anticipation, adaptation and dynamically seeking ways to support users.

Although agents can be a very powerful technology - especially for users who need to be flexible and do not wish to explicitly instruct the computer - but, they increase the systems complexity and this may undermine the benefits of software agents. In the other word, agents can shield users from complex interactions by anticipating their actions which may actually decrease users situational awareness and leave them uncertain as to what is being done on their behalf. This is a consideration that developers of the technology need to take into account.

### 5.9.1 Situation Awareness and Decision Making

The research by Endsley (2000) addresses the issues of why application of software agents in an emergency response task may decrease users' situational awareness.

Endsley (2000) defines situational awareness (SA) as “perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future”. In fact Endsley (2000) believes that SA is gained through three separated levels: Perception, Comprehension, and Projection.

Endsley (2000) argues that the perception level is fundamental in that first cues are gain by the users and without this basic perception of important information, the odds of forming an incorrect picture of the situation increase dramatically.

At the comprehension level, according to Endsley (2000) situation awareness is a construct that goes beyond mere perception and this level encompasses how people combine, interpret, store, and retain information. The comprehension level includes more than perceiving or attending to information, but also the integration of multiple pieces of information and a determination of their relevance to the user’s goals.

At the highest level of SA, Endsley (2000) points out that the ability to forecast future situation events and dynamics is the attribute of the people who have the highest level of understanding of the situation. This ability to project from current events and dynamics to anticipate future events and their implications allows for timely decision making. In fact it is mark of a skilled expert.

As the result, if the software agents act as a shield between users and systems, then they can potentially affect the different levels of situational awareness such as ‘perception’ and consequently perfume as barrier to SA instead of a facilitator in a dynamic environment.

In fact it is important to remember that users are able to construct their own goals and values, then decide, plan and act in ways to help these achieve goals and values. So it is possible that users fail to understand what is happening within a system or when they cannot control the system because their autonomy is being reduced via agents or the system relies on the agents have unpredictable behaviours. Payne et al. (2000) believe that deskilling may also occur when the agent makes decisions for the users rather than just providing advice, or if the user is prevented from make the wrong decisions.

These difficulties can be compounded where multiple agents and humans are required to work as a team in a highly dynamic environment. In an evolving dynamic environment such as emergency response tasks, there are usually issues of time pressure, conflicting sub-goals, division of labour amongst subordinates, and allocation of resources. In such an environment humans face complex situations in which they often lack sufficient knowledge, skills, and time to perform their tasks. In these environments, commanders have a sensitive task and great responsibility to achieve their goals in the best and most reliable way.

According to Wallenius (2004) command and control is the act of fulfilling a task assigned to an organization in terms of designing, evaluating, approving, and executing, a solution on a lower level of abstraction. To fulfil these tasks, a commander should follow a series of mental and cognitive model. Yufik (2003) describes the following process by which C2 make decisions; first they comprehend their environment by assessing the distribution of their resources and threats. Afterward, they start assessing their situation and get aware of it, which concluded by forming an associated network in commander's memory accounting for all units and their interactions. Through these steps they can cut down the psychological complexity of the allocation problem and increase their ability to solve it quickly and accurately.

This process emphasizes the fact that, in dynamic environments, commanders must deal with distinctive and situation specific factors such as non-quantified information, complex or vaguely specified mission objectives and dynamically changing situations affected by incomplete, changing, new information, obstacles, and other actions. Therefore the interaction of the human – particularly decision makers – with their operation environment has a significant impact on their decisions that concluded from the means they sense and get aware of their situations.

As Endsley (2000) describes when the environment is dynamic, certain aspects make an important contribution to the third level of human situation awareness, Projection, that are necessary for coping with unpredictable environment. In these situations, the rate at which information is changing is an important factor in the awareness of the current situation, which determins the ability to project into the ofuture situation.

The dynamic nature of a situation dictates that, as the situation is always changing, so must the person's situation awareness constantly change or be rendered outdated and thus inaccurate. In highly dynamic environment, this forces the human operator to adapt many cognitive strategies for maintaining situation awareness. This approach reflects the fact that situation awareness is derived from a combination of environmental entities such as system's interface and functionality and other team mates and so on, as integrated and interpreted by individual decision makers (Figure 5. 11)

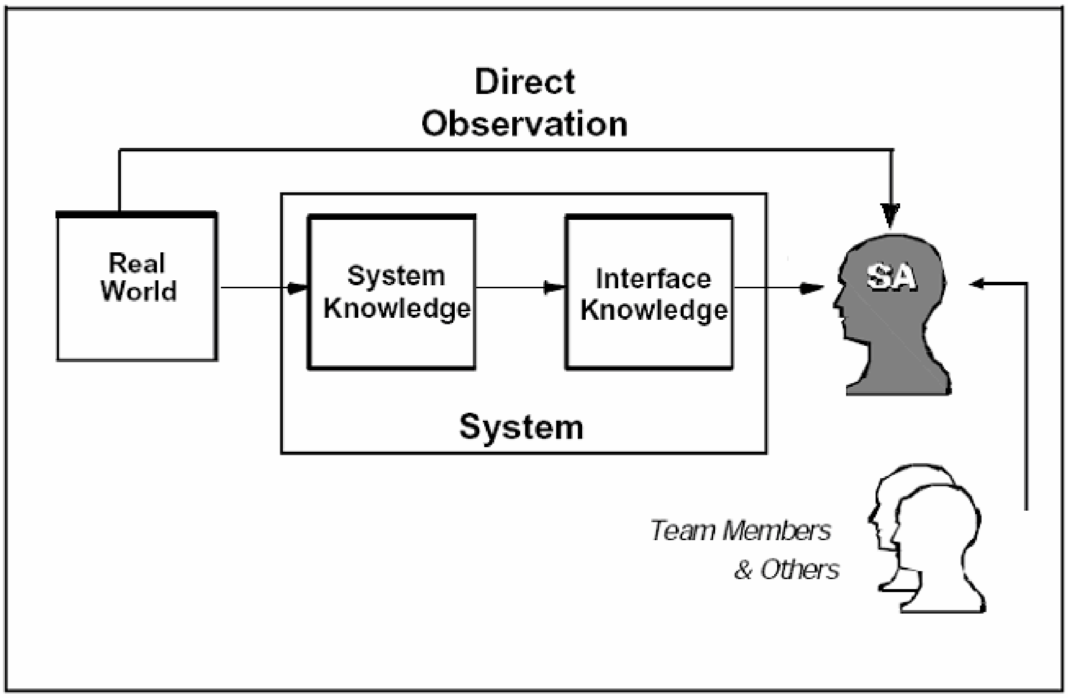


**Figure 5.11** Source of situation awareness information (Endsley, 2000)

In fact Endsley (2000) strongly believes that situation awareness is the main predecessor to decision making and there is a strong relation between decision making and situation awareness. This integral relationship is the bottom line for decision makers that their decisions are formed by their awareness of the situation and, their situation awareness is formed by their decisions. As the result the proper actions (orders, signals, movements, …) will be taken place concerning to the decision is being made (Figure 5.12)

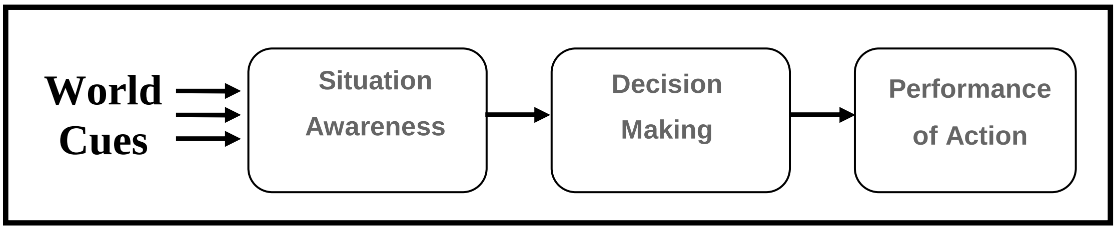


**Figure 5.12** Cognitive Processes of an Action (Endsley, 2000)

SA also depends on the other means that human get information and process them. One important factor that significantly affects the human SA is the operation goals. Goals are central to the development of situation awareness. Endsley (2000) believes that human information processing within complex systems is seen as altering between data driven and goal driven processing. In goal driven processing, attention is directed across the environment in accordance with active goals. The operator actively seeks information needed for goal achievement and goal simultaneously acts as a filter in interpreting the information that perceived. In data driven processing, perceived environment cues may indicate new goals that need to be active. According to Endsley (2000) the dynamic switching between these two processing modes is important for successful performance in many environments.

This perspective of SA emphasizes that in the situations like the public safety operations and emergency first response tasks, the situational awareness is central to the success of tasks particularly in dynamic environments. Because it is derived from the objectives of operations and also the ways human mind tends to gain and process the information. So, any technology which is associated with helping users and decision makers cope with the uncertainties of dynamic environments should be aligned with the users' situation awareness requirements.

Existing technological systems do not provide situation awareness in and of themselves. It takes a human operator to perceive information to make it useful and the role of technology is to help to get accurate and enough perception of their environment at the right time.  This is the point expressed by Wallenius (2004) that situation awareness is a mental state and cannot be directly interacted with by use of technology. Therefore any technology or model related to SA should provides means to externalise it to, in turn, facilitate sharing it over a computer network and interacting with it through the different support tools.

It can be concluded that any technology that can augment the effectiveness of operations in critical situations, it should be built based on the notion of affecting the right “cognition”, in the right agents, at the right time instead of simply transmitting data. Nosek (2004) spells out that such a technologies must dramatically improve anytime, anyplace collaboration work by better managing the social, cognitive, and procedural complexities inherent in joint work. These technologies must substantially improve the process of establishing and maintaining shared task understanding and situational awareness “naturally” from wherever and whenever the work needs to be done.

### 5.9.2 Sensemaking in a Changing Environment

Although SA seems to be essential to a decision maker’s success, there are other significant mental and cognitive issues that contribute in this process. In time critical and high pressure environments not only should decision-maker get aware of their situation, they must also understand the issues, make sense of the environment and then take proper actions all in a very short period of time. Potts (2003) describes a C2 process as an adaptive process consisting of number of interacting elements. According to Potts (2003), among these element, awareness, understanding, and sensemaking are those that playing a vital role for any present and future decisions and actions.

Potts (2003) states that awareness is the quality that the cognitive domain brings to the information provided by monitoring technologies. It is a filtration of this information by the cognitive process that relies on the previous knowledge and beliefs about the current situation. Understanding follows awareness and it is the ability of the brain to correctly perceive the current situation and to understand its significance, based on the filtered information means. According to Potts (2003) once understanding has been achieved, sensemaking can take place. This is the process by which an understanding of the current situation is connected to a sense of how the situation might develop, and what activity must take place. The completion of the sensemaking process is the making up of one’s mind and arriving at a decision.

The implication is that without appropriate situational awareness in dynamic environments such as battlefields or rescue operations, , decision makers do not have sufficient understanding of the situation and its context and cannot make proper sense of it. Inadequate situational awareness limits the ability both to observe and perceive the situation adequately and in such cases becomes a sensemaking constraint. Therefore the SA and understanding are the precursor of the concept of sensemaking which  critically affects the work of decision makers in dynamic environments.

There are many definitions constituted as the definition of sensemaking throughout the literature (Wieck et al., 2004; Waldrop, 2003; Nosek, 2004; Nosek, 2005).

Many tools such as data mining technologies help only to collect and refine the data and some others help only to share clues but neither approach helps connect the data or pieces together an understanding of what a future situation would be. Waldrop (2003) consider this as perhaps the most difficult aspect of sensemaking that is working from fragmentary clues to develop an understanding of the how and why of a situation might be.

Weick et al. (2004) believe that the sensemaking is central to any action because it is the primary site where meanings materialize that inform and constrain identity and action. Viewed as a significant process of organizing, Wieck et al. (2004) state a central theme in both organizing and sensemaking is that people organize to make sense of equivocal inputs and pass this sense back into the world to make that world more orderly.

Wieck et al. (2004) argue that sensemaking is about the interplay of action and interpretation rather than the influence of evaluation on choice. When action is the central focus, such as in emergency response task situation, interpretation, not choice, is the core phenomenon. So, when the situation gets more complex and dynamic, finding proper and timely solutions for a particular issue, highly depends on how human can make sense of their environment and get adapt with its changes. Hence, role of the sensemaking become more crucial since it significantly affect the following actions that, in turn, could have a considerable impact on the operation outcomes.

According to Nosek (2004) in complex environments, where not all variables and relationships are known, humans create rather than discover their future. They create the future by receiving and understanding the information within their environment and then acting correspondingly. The subsequent actions, including probing of the environment leads to changes in the environment. These changes must provide meaningful input for other agents, both human and non-human. Human and non-human agents must be attuned to relevant signals and information, to act based on them, and to probe for additional relevant information. This is what is described by Weick et al. (2004) as the immediate stage that happens after the sensemaking process takes place.

Many of the first emergency response tasks and military operations heavily rely on the teamwork and collaboration performance. Research in this area entails a careful understanding of the sensemaking process in the collaborative work environment. Adding to this point, it is important to acknowledge that this collaborative teamwork is supposed to be carried out in atypical extreme environment where environmental factor are subject to rapid change . In such an environment sensemaking should be viewed as the collaborative sensemaking which embrace the individuals' and teams' sense of their environment that could lead them to accomplish their individual and team objectives and goals. In a collaborative sensemaking, participants follow a series of rules concerning the means they can make sense whatever related to their mission.

Nosek (2005) notes that in collaborative sensemaking participants accept that data discovery will be incomplete; that their efforts to comprehend, interpret, and integrate data will be difficult and inaccurate to some degree; and that their actions that emerge from sensemaking will fail in some ways and alter the situation in some unknowable way.

As discussed earlier, some technologies such as mobile agents can augment individuals and group SA and consequently the sensemaking, but it is important to note that every technology supposed to support the better sensemaking should be along with the human's sensemaking criteria. As Nosek (2005) points out, existing technologies focus on sharing data and not on supporting the sensemaking activities of participants engaged in a collaboration. Technology must fully support the sensemaking activities of participants who engage in various collaborations.

The way to build better sensemaking technologies is to understand the strengths and limitations of human sensemaking, that is, the strengths and limitations of how participants discover the right signals at the right time, make sense of them, and transmit signals to other participants at the right time as they collaboratively construct sufficient meaning to act. Therefore, technological advances are not just about the technical ways of providing huge amount of information rather they should act as a sort of tools that could empower humans' ability of sensemaking. Suitable criteria that could fulfil this aim are introduced by Nosek (2005) through the Collaboration Envelopes ™ architecture that wrap around sensemaking processes and build more cohesive architectures to fully support sensemaking processes. As Nosek (2005) explains in designing any technology it is critical to remember that processing of sensemaking needs to occur at the individual level to support that of the team.

According to Nosek (2004; 2005) process of sensemaking in individual level comprise of three major elements: Signal In, Signal Out, and Constructing Meaning.
Signal In is a boundary object and it is something external to the cognitive domain and observable by an agent. This signal affords action opportunity to a class of agents of similar capabilities. The main characteristics and conditions for this signal are:

1. It must be received at the right time;
2. It must be received from the right agent/s;
3. It may be actively pulled in by the receiving agent, including action by the receiving agent to uncover/clarify signals;
4. It must have sufficient signal strength, that is, the inherent properties of the signal to project clearly over the noise in the environment;
5. It is affected by receiving agent factors such as: sensing capabilities, cognitive workload, working memory capacity, goals, and hypotheses.

Signal Out is the action or the constructed boundary object (something an agent consciously or subconsciously externalizes, like a message, picture, gesture,

A Signal Out:

1. May or may not be attended to by other agents;
2. Must be generated at the right time;
3. Must be directed to the right agents while denying it to the wrong agents;

Also a Signal Out transmitted by the sending agent, is affected by such factors as:

- The degree to which a sending agent evaluates that receiving agents do not share the same meaning of a situation, the effort to transmit,
- The available means to transmit,
- The perceived effectiveness of means,
- Trust of receiving agents, dependence on receiving agents to accomplish sending agents' goals,
- Task importance,
- Time to achieve shared meaning,
- Task ambiguity, and so forth.

Some factors that affect the processes of constructing meaning or the make sense of a received signal include:

- Available knowledge to process signal, that is, the episodic nature of elicited/accessible knowledge
- Task importance to which the signal is related;
- Some cognitive limitations related to such as cognitive workload, working memory capacity, goals, and hypotheses;
- Beliefs, trust in origin, and dependence on others

The relation between the elements of sensemaking at individual level is depicted in the Figure 5.13.

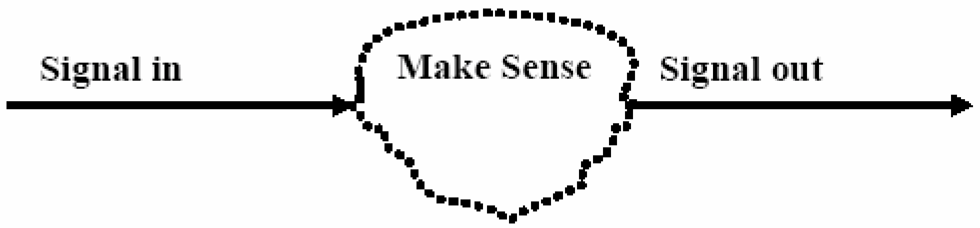


**Figure 5.13** Single Sensemaking Cycle (Nosek, 2005)

While many individual agents within an aggregate can be processing the same signal at the same time, although not necessarily in the same way, the aggregate, like a team or organization, cannot process a signal. In fact, within a collaboration, agents must be aware of important Signals Out at the right time, and at the same time, be open to important signals coming from another collaboration to shift attention at the right time. In such a situation the technology must help the sensemaking cycles be linked among individuals within a team, then team link the results of their sensemaking cycles to other teams in the organization by linking with one or more agents of those teams, and the organization link their sensemaking cycles to agents within other organizations as shown in the Figure 5.14 (Nosek, 2005). This could help to achieve a better and more meaningful sensemaking over the whole organizations who involve in collaboration in individual, team, and organizational level.

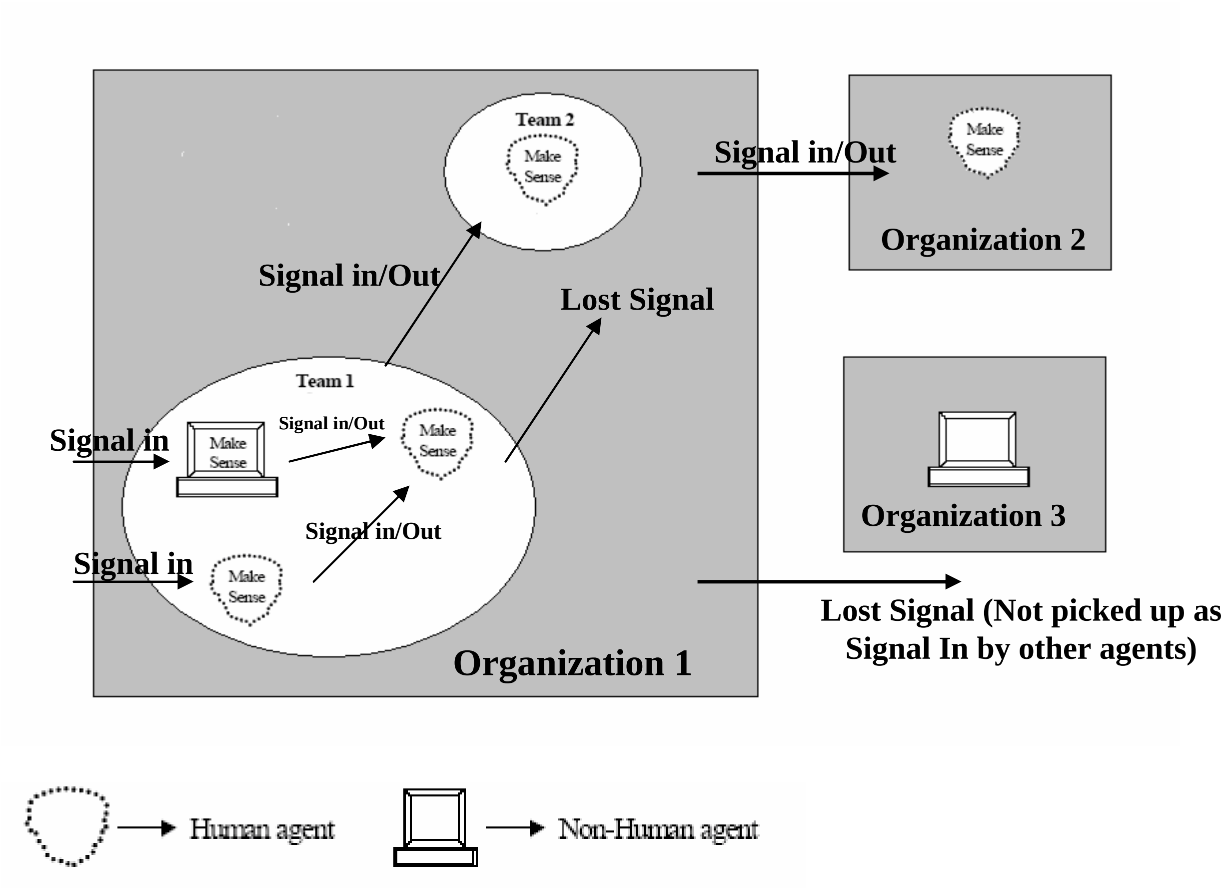


**Figure 5.14** Sensemaking cycle and linkages (Nosek, 2005)

### 9.5.3 Knowledge and Sensemaking

One important factor that contributes in the sensemaking is the knowledge of agent who makes sense of its situation and environment. Based on the knowledge agents for each moment or episode of situation they can adopt proper decision leading to a corresponding action. As mentioned earlier, Nosek (2005) expresses that in the Constructing Meanings stage of sensemaking process, the available knowledge is an important factor for the agent. Each agent has an "effective" knowledge of the situation that can be different from other agents who participate (Nosek, 2004). This knowledge is available in the agents' memory and it is episodic, which means the knowledge shifts with signals received and as the result the available for processing signals within working memory at a given time changes.

Knowledge plays a key role in the sensemaking process and managing knowledge could help different agents in a same situation have a similar or even close sense of a particular situation. Achieving this goal could be very crucial for the situations where the environment is highly dynamic and timely decisions are critical. To achieve this target, tools and techniques that can embrace both technical and social aspects are promising. That means agents' (human and non-human) knowledge needs to adopt complementary approaches and have the same or a close level of understanding to avoid any sensemaking that may contradictory.

#### 5.9.3.1 Role of Knowledge Management in the Sensemaking Process

Knowledge management techniques seem have the great potential to deal with these issues. According to Nitto et al. (2002) knowledge management (KM) is widely recognized as a critical tool in any kind of organization. It has to do with structuring information, ensuring that it is available to all potential users, easily accessible, and presented in such a way that all data relevant to the requesting users are effectively returned in a reasonable amount of time. Also Nonaka and Nishiguchi (2001) studies show that knowledge management concerns the communications of individuals in a social context by which knowledge could transfer among its different forms (Tacit or Explicit).

This approach to knowledge and knowledge management is a close fit to the characteristics of the sensemaking. Dervin (1999) spells out that sensemaking focuses on the human individual but it does not rest on an individualistic theory of human action. Rather, it assumes that structure, culture, community, organization are created, maintained, reified, challenged, changed, resisted, and destroyed in communication and can only be understood by focusing on the individual-in-context, including the social context.

He sees sensemaking within a triangle, which encapsulates the picture of the human (individually or collectively) moving from a situation (time-space) across a gap by making a bridge, and then moving onto the other side of the bridge and get to a new situation. The three points of this triangle, therefore, are situation, gap/bridge, and outcome (Figure 5.15).

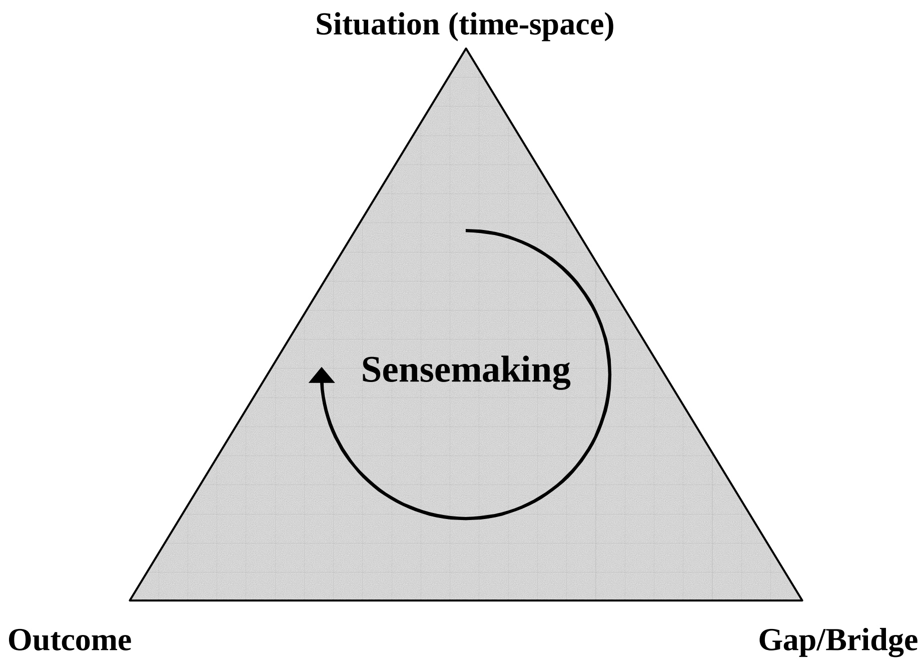


**Figure 5.15** The sensemaking triangle (Dervin, 1999)

Nosek (2004) also expresses that sensemaking is the process whereby people interpret their world to produce the sense that shared meanings exist. Sensemaking occurs and can be studied in the discourses of social members rather than simply occurring in their mind and the socially constructed object, or facts, of the world exist through and are located in the discursive sensemaking of members. Moreover , Weick et al. (2004) argue that communication is a central component of sensemaking and organizing. They see communication as an ongoing process of making sense of the circumstances in which people collectively find ourselves and of the events that affect them. Sensemaking, to the extent that it involves communication, takes place in interactions in order to share understanding means and to lift unclear knowledge out of the tacit, private, complex, random, and past to make it explicit, public, simpler, ordered and relevant to the situation at hand.

The above views ofsensemaking imply that knowledge management outcomes have strong ties with the individual and organizations sensemaking. Awazu (2000) have a strong stand on this notion and draws a very tiny line between sensemaking and knowledge. Awazu (2000) believes that sensemaking is a knowledge management activity and it refers to the comprehension of retrieved knowledge and the process of recognizing the context around knowledge and is either conducted through the use of schemas and metaphors or is based on habitual interpretations and behavioural episodes. According to Awazu (2000) sensemaking is important capability for any organizations, since it integrates people's thoughts and generates new knowledge. This is a particularly crucial point when any sensemaking and the ensuing decisions involve safety and human lives.

## 5.10 Chapter Conclusion

This chapter has presented technological, and human, characteristics and capability for public safety tasks where the operational environment are characterised by ambiguity, high stress, and time dependency of decision-making. The various technologies and human characteristics have each been described with some indication of how they may influence each other. There is still however the challenge of bringing all technological and human aspects together to provided an effective holistic programmed for co-ordinated reponses.

In the next final chapter of the thesis conclusions will be drawn in order to identify how technologies such as mobile agents and wireless communications can operate as complementary components helping decision makers get to more reliable, more accurate and timely decisions matching and aligned the environmental uncertainties and its rate of change.

# Chapter 6

# Conclusions

## 6.1 A Summary of the Results and Conclusions

The major thrust of this thesis has been to investigate the contribution that mobile agent technology and wireless communication systems can make to the sense-making of decision makers who are responsible for accomplishing critical assignments in an extreme environment. The study focused on the specifications of both technologies in order to find out what features are significant and promising in the context of the research question: *'How the particular attributes of mobile agents and capabilities of new wireless radio technologies can help decision makers to get a better understanding and knowledge of their environment, become more aware of their situation and make sense of the operations' conditions in order to make more precise and timely decisions in extreme situations?'*

A case study methodology was used for the study since it required the answering a 'how' question, as recommended by Yin (2003). Due to the difficulties of collecting primary data, a secondary case approach was used for study. A suitable secondary case for which there is abundant data is the fall of the World Trade Centre in New York on September 11 of 2001.This case is a prime example of events that unfolded in a high stress, dynamic and unpredictable environment, where decision makers had to make crucial decisions amid extreme environmental conditions and ambiguities. As a result, many of these decisions are made with insufficient relevant information and little known about their consequences including their considerable impact on the life of others.

Considering the research question: *'How the particular attributes of mobile agents and capabilities of new wireless radio technologies can help decision makers to get a better understanding and knowledge of their environment, become more aware of their situation and make sense of the operations' conditions in order to make more precise and timely decisions in extreme situations?'* , this study reveals that many of the uncertainties that decision makers face in extreme environments, where there are urgent issues of public safety, are deeply dependent on accurate and timely local and general information of the operational environment. In fact, humans need to receive, filter, process and make sense of the environmental information and derive a decision based on what they perceive of the environment and according to the resources they have available. They then act to follow through on the decision.

The challenge is that information in a fast changing environment is continually being created, changed and made obsolete so fast, making it difficult for decision makers to properly keep abreast of the situation. On the other hand, humans are capable of rapidly assessing their situation on the basis of the latest information they have received. They are also flexible enough to revise this awareness by updating their information from different sources. However, they may fail to receive accurate up-to-date information to become properly aware of their situation if they do not capture the right signals from the right source at the right time. Hence, public safety personnel are not able to make sense of their operation environment correctly. Consequently, the decisions they make, which are built on their understanding and sensemaking of their environment, may fail, since they are not based on complete information. Without the right support, operational decisions cannot be made at the same pace or at the same level as the variations in the environment.

Evidence from this study shows that mobile agent technology can address these issues by taking advantage of the advances in software agent concepts. In this type of networked mobile setting they can act as autonomous entities in order to provide a better paradigm of information processing and information exchanges in a dynamic environment. Mobile agents can handle many critical tasks by sensing and measuring environmental factors through an appropriate network of sensors and data visualisation. In addition, they can make local decisions, and act on the behalf of users thus reducing the cognitive load of operational information and providing decision makers with the sort of information they require in a right time.

The findings of this study also show that new wireless technologies are able to handle high rates of data in an infrastructure free environment. Therefore, the combination of mobile agent technology and wireless communication systems can provide an ideal system for the first emergency response and military operations, where workers are involved in environments which are highly dynamic and the role of information is crucial. To be effective, these technologies should support human cognitive requirements in order to augment the effectiveness of their critical decisions.

In fact, mobile agents moving through a ubiquitous wireless network – such as a meshed Ultra Wideband wireless sensor network – can consistently scan the operation environment, based on the mobile users' profile and needs, providing them with more reliable information about their surrounding environment in a timely fashion. This can increase the degree of users' situational awareness and sensemaking of the environment. Users will also be able to refer to their episodic knowledge, revise their information and make decisions based upon new knowledge, with reduced cognitive burden, less ambiguity and less mental pressure, leading to more constructive actions.

Referring back to the research question, the research findings and results explicitly show how the applications of mobile agents and new wireless technologies can help the decision makers to understand and make sense of the extreme environments, making appropriate decisions and courses of actions. Consequently, they would be able to deal properly with the life-sensitive and unpredictable situations particularly in the public safety operations. The technologies have studied in the light of human sensemaking requirements and the research has analysed the factors contributing to human cognitive states especially in time critical situations.

## 6.2 Further Work

This thesis has addressed a number of significant issues associated with decision making and information dissemination in high stress and dynamic environments. However, there are still a number of issues that require further investigation. These are described below:

- The role of the mobile agents in conjunction with wireless technology described in chapter 4 and chapter 5 require knowledge of how mobile agents can handle information and move through the wireless network. This is achieved through understanding the characteristics of mobile agents and the applications introduced throughout the literature. Further work should consider the effect of the mobility of the nodes on mobile agents existing in a wireless technology and the way they can handle information in a mobile setting. Furthermore, what mechanisms may be utilised to couple mobile agents with wireless communication technologies in a meshed configuration are issues worthy of study.

- In chapter 4, this thesis introduced the key role of mobile agents in fulfilling the general requirements of public safety operations. The advantages described there concern the way mobile agents and wireless technology can help humans to cope with environmental uncertainties. Following this idea, there are many issues relating to the security of information travelling through the networks and the means by which mobile agents could affect this security. Thus, there exists a potential for work in the area of security issues of public safety and the roles that mobile agent could play in this area.

- To date, there has been little work on the effects of mobile agents on the decisions made by decision makers in a fast changing environment. Most of the work done to date relates to the application of static agents and to some degree mobile agents, in situations where environment are changing gradually. Much of this work concerns issues of knowledge management in organisations where the speed of change is notably slower than civilian or military emergency situations. In organisations requirements for mobile agents are identified based on their users' profiles, which do not change quickly or the changes are only partially. But in an emergency first response task, mobile users' profiles may change frequently in many areas according to the demands of an ever-changing environment. Hence, there is a potential to conduct further study of these unstable profiles and the means by which mobile agents cope with these changes.

- In chapter 5, the study introduced the human sensemaking process and the specifications of these procedures. Studies in this area have been mainly carried out based upon human sensemaking in an organisation, where the rate of change is slow compared to that in extreme environments. Many of these concepts may be applicable in both fast and slow changing environments. There may be value in further study of Nosek's 'signal' idea in a dynamic environment, referenced in Chapter 5. Some efforts in this direction are demonstrated in the paper, attached in the appendix, and are submitted by the candidate and his supervisor to an upcoming conference.

# Bibliography

3COM 2003, *Deploying 802.11 Wireless LANs*, White Paper, [online] Available: www.3com.com. [Accessed 18 October 2004].

Albowicz, J. et al., 2001,'Recursive position estimation in sensor networks', *Proceeding of IEEE International Conference on Network Protocols*, Riverside, California, pp35–41.

Alexander, B & Snow, S 2002, 'Preparing for wireless LANs', *Packet Magazine (Cisco System)*, Vol. 14, No. 2. pp.36-40.

Amet, A. et al., 2003,'Ultra Wideband Technology for Aircraft Wireless Intercommunications Systems (AWICS) Design', *Proceeding of the IEEE Conference on Ultra Wideband Systems and Technologies*, November 2003, Reston, VA.

Ametller, S., Robles, M. E. and Ortega-Ruiz, P. 2004, 'Self-Protected Mobile Agents', *Proceeding of Third International Joint Conference on Autonomous Agents and Multiagent Systems , Volume 1 (AAMAS'04)*, New York City, New York, USA

Arensman, B. 2003, *Unleashing UWB:Ultra-wideband may become the next big wireless technology, but its commercial success depends on the outcome of a contentious standards battle*, REED BUSINESS INFORMATION, [online] Available: http://www.wirelessweek.com/index.asp?layout=articlePrint&articleID=CA319077 [Accessed: 13 November 2004].

Artimi, 2003, *UWB and Mesh Network*, White Paper, Artimi Ltd., [online] Available: http://www.artimi.com/ [Accessed: 24 October 2004]

Avison, D. E., Lau, F., Myers, M.,Nielsen, P. A. 1999, 'Action research', *Association for Computing Machinery. Communications of the ACM,* January ; Vol. 42, No. 1, pg. 94(5).

Avison, D. E., Myers, M. 1995, 'Information Systems and Anthropology: An Anthropological Perspective on IT and Organizational Culture', *Information Technology & People*, Vol. 8, No. 3, pp43-56.

Awazu, Y. 2004,' Knowledge Management in Distributed Environments: Roles of Informal Network Players', *Proceedings of the 37th Hawaii International Conference on System Sciences* , USA.

Baskerville, R. & Wood-Harper, A. T. 1998, ‘Diversity in information systems action research methods’, *European Journal of Information Systems*, Vol. 7, 90–107.

Baskerville, R. L. 1999,’Investigating Information Systems With Action Research’, *Communications of the Association for Information Systems*, Article 19, Vol. 2, October.

Bing, B. (eds.) 2002, *Wireless local area networks : the new wireless revolution* , Wiley-Interscience, New York.

Blankenbeckler, A. 2002, *An Introduction to Bluetooth*, Wirelessdevnet, [online], Available:http://www.wirelessdevnet.com/articles/bluetooth.html [Accessed 2 September 2004].

Bock, W (2003), *Lessons from September 11*, media release, The digital age storyteller, USA, [online] Available: <http://www.mondaymemo.net/020909feature.htm> [Accessed 3 January 2005] .

Boukerche, A. & Nelem, P. R. W. & Araujo, R. B. 2004, ‘A Fast and Reliable Protocol for Wireless Sensor Networks in Critical Conditions Monitoring Applications’, *ACM* , October, pp. 157-164.

Bradshaw, M.J (eds.) 1998, *Software Agents*, AAAI Press, Cambridge, Massachusetts.

Broersma, M. 2004, *Mesh: The next step for wireless, technical report*, ZDNet UK, [online] Available: <http://insight.zdnet.co.uk/communications/wireless/0,39020430,39149930,00.htm> [Accessed 10 January 2005].

Broersma, M. 2004, *Mesh: The next step for wireless*, ZDNet UK, [online] Available: http://insight.zdnet.co.uk/communications/wireless/0,39020430,39152270,00.htm [Accessed : 11 September 2004].

Brown, B., Morris, P., and Thompson, C. 2003, ‘SUO Communicator: Agent-based Support for Small Unit Operations’, *Proceeding of International Conference of Integration of Knowledge Intensive Multi-Agent Systems*, 30 September, USA.

Callaway, E. H 2003, Wireless Sensor Networks - Architectures and Protocols, Auerbach, Boca Raton, Florida.

Careless, J. 2002, *The recovery continues* [online] Available: http://mrtmag.com/mag/radio_recovery_continues/ [Accessed 4 January 2005].

Caripe, W., Cybenko, G., Moizumi, K., and Gray, R. 1998, ‘Network awareness and mobile agent systems’, *IEEE Communications Magazine*, July, pp 44–49.

Chamberlain, K. 1995, *WHAT IS GROUNDED THEORY?*, Principia Cybernetica [online] Available: http://kerlins.net/bobbi/research/qualresearch/bibligraphy/gt.html [Accessed: 21 December 2004].

Chapman, T. 2002, *Short Range Wireless*, Roke Manor Research, [online], Available: www.roke.co.uk [Accessed 25 January,2005].

Chen, K. 1994,’Medium Access Control of Wireless LANs for Mobile Computing’, *IEEE Network*, September / October.

Child, J. 2003,’Wearable Computers Blaze Connectivity Path’,*COTS Journal*, April, pp.14-18.

Commtech 2003, *Can’t We Talk? Interoperability, Working Together To Bridge the Communications Gap To Save Lives A Guide for Public Officials*, National Task Force Publication under the Agile Project Programme, (brochure), USA.

Corson M. S., Macker, J. 1996, ‘*Reliable Scalable Multicast and a Self-Organizing Approach for Long-Lived Sessions’*, Technical Report.

Couper, C. 2004, City-Net: The future of wireless, *Computer World*, [online] Available: http://www.computerworld.com/mobiletopics/mobile/story/0,10801,89492,00.html?SKC=mobile-89492 [Accessed: 13 February 2005].

Cox, J. 2003,’Bluetooth gets greasy and gritty’, *Network World*, July, p. 14.

Craig, W. C. 2004, *Zigbee: “Wireless Control That Simply Works”* , ZMD America, Inc. [online] Available: www.ZMD.com [Accessed 10 February 2005].

Crawford, I.M. 1997, Marketing Research and Information Systems, *Proceeding of Food and Agriculture Organization of the United Nations conference*, Rome,

Creswell, J. 1994, *Research Design, Quantitative and Qualitative Approaches*, Thousand Oaks, California, Sage.

DARPA (2004) , DARPA Advanced Technology Office, Accessed 23 August 2004, <http://www.darpa.mil/ato/programs/suosas.htm>.

DARPA 2001, *A Remote Ecological Micro-Sensor Network*, [online] Available: http://www.botany.hawaii.edu/pods/ [Accessed 13 January 2005].

Davidson, A.L. (2002), ' Grounded Theory' , PageWise Inc., [online] Available: http://az.essortment.com/groundedtheory_rmnf.htm. accessed: 14 November 2004

De, S., Qiao, C., and Wu, H. 2003,'Meshed multipath routing with selective forwarding: An efficient strategy in wireless sensor networks', *Elsevier Computer Networks, Special Issue on Wireless Sensor Networks,* Vol. 43, No. 4, pp. 481–497.

Dees, T. 2000, *Information and Communications Technology for Public Safety*, [online] Available: http://www.timdees.com/articles/icma.htm [Accessed 14 September 2004].

Dervin, B 1999,'Chaos, Order, and Sense-making: A Proposed theory for information design', in Jacobson, R (eds.), *Information Design*, The MIT Press, Cambridge, Massachusetts.

Du, T. C., Li, E. Y., and Chang, A. 2003, 'MOBILE AGENTS IN DISTRIBUTED NETWORK MANAGEMENT', *Communications of the ACM*, July, Vol. 46, No. 7,pp127-132.

Dunsmuir, A. and Williams, L. 1991, *How to do Social Research*. Collins, London

Eisenhardt, K. M. 1989, 'Building Theories from Case Study Research', *The Academy of Management Review*, October, Vol. 14, No. 4, pg. 532.

Endsley, M. R. 2000, 'Theoretical underpinnings of situation awareness: A critical review', in Endsley, M. R.&. Garland, D. J (eds.), *Situation awareness analysis and measurement*. Mahwah, NJ.

Etzioni, O., and Weld, D. S. 1995, 'Intelligent Agents on the Internet: Fact, Fiction, and Forecast', *IEEE Expert*, Vol. 10, No. 4, pp.44–49.

Evan, N. M. R. & Chandler, M. & Nobel, K. R. 2002, 'Threat Response: a Compelling Application for Wearable Computing', *Proceedings of the 6th International Symposium on Wearable Computers*, IEEE Computer Society, Seattle, Washington.

Feldman P. M. 1998, *Emerging Commercial Mobile Wireless Technology and Standards: Suitable for the Army?* , RAND, [online] Available: http://www.rand.org/publications/MR/MR960/index.html#contents [Accessed: 4 October 2004].

Flickenger, R. 2003, *Wireless Hacks*, O'Reilly & Associates Inc., USA.

Flood, G. and Whittle, S 2004, *From Mesh to UWB: Untangling the wireless future*, ZDNetUK , [online] Available: http://insight.zdnet.co.uk/communications/wireless/0,39020430,39152270,00.htm [Accessed 10 September 2004].

Foner, L. 1993,*What's an Agent, Anyway? A Sociological Case Study*, MIT, [online]: http://foner.www.media.mit.edu/people/foner/Reports/Julia/Agents--Julia.pdf, [Accessed: 3 October 2004].

Foner, L. 1997,' Entertaining Agents: A Sociological Case Study', *Proceeding of the First International Conference on Autonomous Agents'*, Marina del Rey, California, pp. 122-129

Fontana, R. et al., 2002,' RECENT ADVANCES IN ULTRA WIDEBAND COMMUNICATIONS SYSTEMS', *Proceeding of the IEEE Conference on Ultra* Wideband Systems and Technologies, Baltimore, MD.

Fontana, R.J. 2004, '*Recent Developments in Short Pulse Electromagnetics or UWB the Old-Fashioned Way ?*', Presented to Microwave Theory and Techniques Society, Northern VA Communications Society 9 March 2004

Frank, R. (2004) Move Over, Bluetooth; ZigBee is here Reed Business Information, [online] Available: http://www.designnews.com/article/CA387448.html [Accessed 2 November 2004].

Franklin, C. 2003, *Introduction to How Bluetooth Works*, HowStuffWorks Inc. [online] Available: http://electronics.howstuffworks.com/bluetooth.htm [Accessed 2 September 2004].

Franklin, S., and Graesser, A.1996, 'Is It an Agent or Just a Program? A Taxonomy for Autonomous Agents', *Proceedings of the Third International Workshop on Agent Theories, Architectures, and Languages.* New York.

Fritz, W. 1996, ' *What Is Intelligence?'* ,New Horizon Press, [online], Available: http://www.intelligent-systems.com.ar/intsyst/intsyst.htm Accessed: 21 December , 2004.

Galeev, M. 2004, *Home networking with Zigbee*, Embedded Systems Programming, [online] Available: http://www.embedded.com/showArticle.jhtml?articleID=18902431 [Accessed 15 October 2004].

Geier, J. 2002, *Wireless LANs*, Second Edition, Sams Publishing, USA

Golmie, N., Cypher, D., Rebala, O. 2004, 'Performance Analysis of Low Rate Wireless Technologies for Medical Applications', *Computer and*

*Communication's special issue on WPANs*, [online] Available: http://w3.antd.nist.gov/pubs/com04_golmie.pdf [Accessed 8 February 2005].

Goodwins, R. 2003, *Mesh standards are thin on the ground*, ZDNet UK [online] Available: http://insight.zdnet.co.uk/communications/networks/0,39020427,2131750,00.htm [Accessed 5 November 2004].

Graue, M.E. 2005, *Introduction to Qualitative Research Methods*, University of Wisconsin-Madison, [online] Available: http://labweb.education.wisc.edu/cni916/def_eth.htm [Accessed : 20 September 2004].

Gray, R.S. 2000, 'Soldiers, Agents and Wireless Networks: A Report on a Military Application', *Proceeding of the PAAM 2000*, Manchester, England.

Greenwood, S. and Nealon, J.L. and Marshall, P. 2003, 'Agent-Based User Interface Adaptivity in a Medical Decision Support System', *Proceeding of the conference in Applications of Software Agent Technology in the Health Care Domain*. Birkhäuser Verlag, Basel, Germany.

Griffin 2002, *Insight into wireless protocols and standards: Crating a secure network for your business, white paper*, Tuanis Technology [online] Available: http://www.tuanistechnology.com/ [Accessed 29 February 2005]

Hamblen, M. 2004, *Ultrawideband: A better Bluetooth*, IDG Communications Ltd., [online] Available: http://cio.co.nz/cio.nsf/UNID/6AD7D5EF0194BC9ACC256EE300156CED?OpenDocument&Highlight=2,Matt,Hamblen [Accessed 16 February 2004].

Harvey, L. J., and Myers, D. M. 1995,'Scholarship and practice: the contribution of ethnographic research methods to bridging the gap', *Information Technology & People*, Vol. 8 No. 3, pp.13-27.

Hernando M. E., Garci F., Perdices F.J., Torralbo V., Gomez E.J., and Pozo F. 2004, 'Intelligent Alarms Integrated in a Multi-Agent Architecture for Diabetes Management', *Transactions of the Institute of Meassurement & Control*. Vol. 26, No.3, pp 185-200.

Hewitt, C. 1986,'Offices are open systems', *Communications of the ACM*, Vol. 4, No. 3, pp271-287.

Hewitt, C., Yonezawa, A. 1977,' Modelling Distributed Systems', *Proceeding of 5th International Joint Conference on Artificial Intelligence*, International Joint Conference on Artificial Intelligence, Cambridge, MA, pp. 370-376.

Heylighen, F. 1993, *Epistemology, introduction, 2004, Principia Cybernetic*, [online] Available : http://pespmc1.vub.ac.be/EPISTEMI.html [ Accessed: 21 December, 2004].

Hofman, M. O., McGovern, A., and Whitbread, K. R. 1998, 'Mobile Agents on the Digital Battlefield', *Proceeding of Second International Conference on AUTONOMOUS AGENTS (Agents '98)*, Minneapolis, St. Paul.

Huhns, M. N. & Seshadri, S. 2000,'Sensors +Agent +Network=Aware Agent', *IEEE INTERNET COMPUTING*, May-June, pp. 84-86.

Huhns, M. N. & Seshadri, S. 2000,'Sensors +Agent +Network=Aware Agent', *IEEE INTERNET COMPUTING*, May-June, pp. 84-86.

Hulter. F and Streeton, G. 2003, *Ultra Wide Band: an overview*, Roke Manor Research, [online] Available: www.roke.co.uk [Accessed: 25 January 2005]

Intel. Corp. 2004, *Ultra-Wideband (UWB) Technology Enabling High-speed Wireless Personal Area Networks*, white paper [online] Available: www.intel.com/technology/ultrawideband [Accessed January 2005].

International Technical Committee for the Prevention and Extinction of Fire 2003, *Annual Report 2003*, Moscow. [online] Available: www.CTIF.org [Accessed 10 October 2004].

Kaplan, B. & Duchon, D. 1988,'Combining qualitative and quantitative information systems research: a case study', *MIS Quarterly*, December., Vol. 12, No 4, p570(16).

Kaplan, B. and Maxwell, J.A. 1994, 'Qualitative Research Methods for Evaluating Computer Information Systems', in Anderson, J.G., Aydin, C. E. and Jay, S. J. (eds.), *Evaluating Health Care Information Systems: Methods and Applications*, ,Sage, Thousand Oaks, California, pp. 45-68.

Karl, R.and Willig, R. 2003, *A short survey of wireless sensor networks Technical Report*, Technical University of Berlin, [online] Available: http://www.tkn.tu-berlin.de/tkn/publications/papers/TechReport_03_018.pdf [Accessed : 10 December 2004].

Karp, B. and Kung, H. T. 1998, *Dynamic Neighbour Discovery and Loop- Free, Multi-Hop Routing for Wireless, Mobile Networks*, Harvard University, [online] Available: http://www.eecs.harvard.edu/~karp/aprl.ps [Accessed: 25 November 2004]

Karp, B. and Kung, H. T. 2000, 'GPSR: Greedy Perimeter Stateless Routing for Wireless Networks', *Proceeding of the 6 Annual International Conference on*

*Mobile Computing and Networking (MOBICOM)*, pages 243--254, Boston, Massachusetts, USA.

King, J. S. 2001, *An IEEE 802.11 Wireless LAN Security* :White Paper', Lawrence Livermore National Laboratory, [online] Available: http://www.llnl.gov/asci/discom/ucrl-id-147478.html [Accessed : 30 November 2004].

Kinney, P. (2003), *ZigBee Technology: Wireless Control that Simply Works*,O'Kane Kinney Consulting LLC, [online] Available: http://www.okanekinneyresources.com/about.html [Accessed 9 January 2005].

Klein, H. K., & Myers, D. M. 1997,'A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems', *MIS Quarterly*, Vol. 23, No. 1, pp. 67–94.

Kling R. 2000,'Social Informatics: A New Perspective on Social Research about Information and Communication Technology', *Prometheus*, Vol. 18, No. 3.

Knight, W. (2002) 'Bullet-proof wearable computer created', *New Scientist*, [online] Available: www.NewScientist.com [ Accessed 12 January 2005].

Kolic, R. 2004, 'Ultra Wideband—the Next-Generation Wireless Connection', Technology@Intel Magazine, February/March.

Kolic, R. 2004, *An introduction to Wireless USB (WUSB)*, Device Forge, [online] Available: http://www.deviceforge.com/articles/AT9015145687.html [Accessed 12 December 2004].

Kotz et al., 2002,'Performance Analysis of Mobile Agents for Filtering Data Streams on Wireless Networks', *Mobile Networks and Applications*, Vol 7, No. pp163–174.

Kotz, D. & Gray, R. 1999,' Mobile Agents and the Future of the Internet', *ACM Operating Systems Review*, Vol. 33, No.3, August , pp. 7-13. Available at: http://www.cs.dartmouth.edu/~dfk/papers/kotz:future2.pdf

Kotz, D., Gray, R., Rus, D. {dfk, rgray, rus}@cs.dartmouth.edu 2002, 'Transportable Agents Support Worldwide Applications', Accessed, 12 August 2004.

Kramer K.H., Minar N., Maes P. 1999, 'Tutorial: Mobile Software Agents for Dynamic Routing', *Mobile Computing and Communications Review*, Vol.3, No. 2.

Lange, D. & Oshima, M. 1999, Seven Good Reasons for Mobile Agents', *Communications of the ACM*, Vol. 42, no. 3, pp 87-89.

Law, C. Mehta, K. and Siu, K. 2001, *Performance of a New Bluetooth Scatternet Formation Protocol*, MIT, [online]. Available:http://www.list.mit.edu [Accessed 20 August 2004].

Lee, A. S. 1989,'A Scientific Methodology For MIS Case Studies', *MIS Quarterly*, March, Vol.13, No. 1, pg. 33.

Lewis, N. 2004, 'Wireless Sensor Networks', in Cook, D.J. and Das, S. K. (eds.), *Smart Environments: Technologies, Protocols, and Applications*, John Wiley, New York.

Lexon, T. et al., 2000,'Task Characteristics and Intelligent Aiding', *Proceeding of IEEE International Conference on Systems, Man, and Cybernetics*, Vol. 2, October, pp. 1123 – 1127, Chicago, USA.

Li, Q. and Rus, D. 2000, 'Sending Messages to Mobile Users in Disconnected Ad-hoc Wireless Networks', *Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking (MobiCOM 2000)*, Boston, Massachusetts, USA.

Liamputtong, P. and Ezzy, D., 2005, *Qualitative Research Methods*, Second Edition, Oxford University Press, UK.

Liu, M. L. 2004, *Distributed Computing Concepts and Application*, Addison Wesley, USA.

Lorincz, K. et al., 2004, 'Sensor Networks for Emergency Response: Challenges and Opportunities', *IEEE Pervasive Computing*, Vol. 3 No.4, p p. 16-23.

Luck, M. and d'inverno, M. 2001, 'A Conceptual Framework for Agent Definition and Development' *The Computer Journal*, Vol.44, No. 1, pp. 1-20.

Macaire, A., Carlier, D., and Paradinas, P. 1999, 'A Personal Agent Manager for Mobile Users',', *Proceeding of the European Multimedia Embedded Systems and Electronic Commerce Conference (EMMSEC'99)*, London.

Maes, P. 1990, *Designing Autonomous Agents.* MIT Press, Cambridge, MA Elsevier, Amsterdam,.

Mann, S. 1998, 'WEARABLE COMPUTING as means for PERSONAL EMPOWERMENT', *Proceeding of International Conference on Wearable Computing ICWC-98*, Fairfax VA. USA

Marci, I. 2003, *802.11 WLAN Security* , Prison TEKLOGIX, [online ] Available: http://www.psionteklogix.com/ [Accessed 18 November 2004].

Marstrande, A. & Hanssen, I. B. 2002, *Ful_llment of Requirements in Public Safety Wireless Communications using TETRA and GSM-R*, Norwegian University of Science and Technology (NTNU), Department of Telecommunications.

Mattisson, S. 2000, *Low-Power Considerations in the Design of Bluetooth*, Ericsson, [online]. Available: http://www.ericsson.com/ [Accessed 20 August 2004].

McCabe, J. D. 2003, 'Network Analysis, Architecture, and Design', Second Edition, Morgan Kaufmann Publishers, San Francisco, USA

McFarland, B. and Wong, M. 2003, 'The Family Dynamic of 802.11', *ACM QUEUE*, [online] Available: http://www.acmqueue.org/modules.php?name=Content&pa=showpage&pid=34&page=5 [Accessed 23 December 2004].

McGrath, S. P. et al., 2003, *ARTEMIS: A Vision for Remote Triage and Emergency Management Information Integration*, Dartmouth University, [online] Available: http://www.ists.dartmouth.edu/library/other/artemis.pdf [Accessed 16 October 2004].

McGrath, S. P., Chacon B., and Whitebread, N. 2000, 'Intelligent Mobile Agents in the Military Domain,' *Proceeding of the Fourth International Conference on Autonomous Workshop on Agents in Industry*, Barcelona, Spain.

Miller, L. E. (2003), *Why UWB? A Review of Ultrawideband Technology*, Report to NETEX Project Office of DARPA, [online] Available: http://www.darpa.mil/ato/programs/netex.htm [Accessed: 25 January 2005]

Milojicic, D. S. 1999, 'Trend Wars: Mobile agent applications', *IEEE Concurrency*, July – September, Vol. 7, No. 3, pp. 80-90.

Montgomery, S. 2004, *Wi.232DTS vs. Zigbee* , Comparing proprietary and standards based solutions, Radiotronix Inc., [online] Available : http://www.radiotronix.com [Accessed 3 January 2005].

Motorola Inc. 2003, *Ultra-wideband, A Wireless Renaissance in the Making*, White Paper, [online] Available: http://motorola.com/semiconductors [Accessed: 8 September 2004].

Motorola Inc. 2004, *Mesh-Enabled Solutions for Emergency Response Agencies* [online], Available: http://www.motorola.com/businessandgovernment/northamerica/en-us/public/functions/browsesolution/browsesolution.aspx?navigationpath=id_804i/id_2523i [Accessed: 21 December 2004].

Muri, F. 1998, *Integrating Intelligent Systems into Human Teams*, University of Carnegei Mellon [online] Available: http://www2.cs.cmu.edu/~softagents/muri/introduction.html [Accessed: 11 October, 2004].

Myers, M. D. 1997,'Qualitative research in information systems', *MIS Quarterly*, Vol. 21, No.2, p241(2).

Myers, M. D. 1999, 'Investigating Information Systems with Ethnographic Research', *Communications of the Association for Information Systems*, Vol. 2, Article 23, December.

Nelson, D. B. (2002), *THE CASE FOR RAPID RE-KEYING*, ENTERASYS Network, [online] Available: wwww.enterasys.com [Accessed 25 September 2004].

Nicopolitidis et al., 2003, *Wireless networks*, J. Wiley, New York.

Nitto, E. D., Pianciamore, M., and Selvini, P. 2002, 'The role pf the agents in knowledge management', *Proceeding of WOA 2002*, Milan, Italy.

Nonaka, I and Nishiguch, T (eds.) 2001, *Knowledge emergence : social, technical, and evolutionary dimensions of knowledge creation*, Oxford University Press, New York.

Nosek, J. T. 2005, 'Collaborative Sensemaking Support: Progressing from Portals and Tools to Collaboration Envelopes', *International Journal of e-Collaboration*, 1(2), 25-39, April.

Nosek, J. T. 2004,'Group cognition as a basis for supporting group knowledge creation and sharing', *Journal of Knowledge Management* ,Vol. 8, No. 4, pp54-64.

Nourbakhsh, I. R. et al., 2005,'Human-Robot Teaming for Search and Rescue', *IEEE Pervasive Computing: Mobile and Ubiquitous Systems*, January, pp. 72-78.

Nwana, H & Azarmi, N. 1997, 'Software Agent and Soft Computing: towards enhancing machine intelligence', *Proceeding of International Joint Conference on Artificial Intelligence*, Menlo Park, California , USA.

Nwana, H. S. 1996, 'Software Agents: An Overview', *Knowledge Engineering Review*, October-November Vol. 11, No 3, pp. 205-244.

O'Brien, R. 1998, *An Overview of the Methodological Approach of Action Research, Web Network*, [online], Available: http://www.web.net/~robrien/index.html [Accessed: 10 February 2005].

Okino, C. 1999, ‘Modeling and analysis of active messages in volatile networks’, *Proceedings of the 37th AnnualAllerton Conference on Communications, Control and Computing*, Allerton, Illinois.

Ordille, J. J. 1996, ‘When Agents Roam, Who Can You Trust?’, *Proceedings of the First Conference on Emerging Technologies and Applications in Communications.* Manchester. UK.

Papaioannou, T. 2000, ‘Mobile Information Agents for Cyberspace – State of the Art andVisions’, *Proceedings of Fourth International Workshop Cooperative Information Agents IV*, Boston, USA.

Patwari, N. et al., 2003,’Relative Location Estimation in Wireless Sensor Networks’, *IEEE Transactions on Signal Processing*, August, Vol. 51, No. 8, pp. 2137-2148,.

Payne et al., 2000, ‘Agent-Based Team Aiding in a Time Critical Task’, *Proceedings of the 33rd Hawaii International Conference on System Sciences.* Hawaii. USA.

Peramanu, D. (2003),*Agent Based Software Engineering :Mobile AgentsDocument Type: Tutorial Report*, University of Calgary

Pham, V. A. & Karmouch, A. 1998, ‘Mobile Software Agents: An Overview’, *IEEE Communications Magazine*, July, pp. 26-36.

Pham,V. A. and Karmouch, A. 1998, ‘Mobile Software Agents: An Overview’, *IEEE Communication Magazine*, Vol. 31, No.7, pp.26—37.

Poor and Hodges 2002, *Reliable Wireless Networks for Industrial Systems*, Technical White Paper, Ember Corporation, 2002 [online] Available: http://www.ember.com/resources/whitepapers/index.html [Accessed: 14 October 2004].

Ray et al., 2003,’Robust Location 14 Detection in Emergency Sensor Networks’, *Proceeding of IEEE INFOCOM*, San Francisco, CA.

Reason, James. 1990, *Human Error*, Cambridge University Press: New York.

Reid, F. & Pasteur, L. 2004, *The Scientific Method*, University of Cincinati [online] Available:http://biology.clc.uc.edu/courses/bio104/sci_meth.htm [Accessed:25 September 2005].

Reilly, D. 2004, *Mobile Agents - Process migration and its implications*, David Reilly, [online] Available:http://www.davidreilly.com/topics/software_agents/mobile_agents/ [Accessed November 2004].

Rogers, M. 2004, No Strings Attached: Wireless Technology Gaining in Popularity, *Florida League of Cities, Inc. [online] Available:* http://www.flcities.com/membership/library_wireless_technology.asp [Accessed 21 September 2004].

Roke Manor Research institute 2004, *Ultra Wideband Communications*, [online] Available: http://www.roke.co.uk/uwb/default.asp [Accessed: 2 February 2005].

Rowe, S. 2003, Ultra *Wideband Cancer Diagnosis: Disease detection goes Ultra wideband*, Roke Mano Research, [online] Available: www.roke.co.uk [Accessed 1 November 2004].

Rupley, S. 2003, 'Wireless: Mesh Networks: These wireless wonders are unstoppable', *PC Magazine*, [online] Available: http://www.pcmag.com/category2/0,1738,4236,00.asp [Accessed 11 August 2004].

Russell, S. & Norvig, P. 2003, *Artificial intelligence: a modern approach*, Prentice Hall, New Jersey.

Sachs, J. et al., 2002,'Digital Ultra-Wideband-Sensor Electronics integrated in SiGe-Technology', *Proceeding of the 5th European Microwave Week (EUMC)*, 23 - 27 September 2002, Milan, Italy.

Santoyo, M. M. 2003, *Wearable Computers Travelling Well*, Synopsys, Inc., [online] Available: http://www.synopsys.com/news/pubs/compiler/compiler.html [Accessed 3 October 2004].

Schoen, R. (Deputy Chief of Medford Police Department) 2002, *Interoperable Communications: Is Mesh Technology the Answer?*, Technical Paper, Police Futurists International , Oregon, Accessed 1 February 2005, http://www.policefuturists.org/newsletter/webarticles/interoperable.htm

Schurr, N. et al., 2003, 'The Defacto Systems: Coordinating Human-Agent Teams for The Future of Disaster Response', *Proceedings of 2nd international workshop on Programming Multiagent Systems*, Melbourne, Australia.

Shen, S. and Norrie, M. 1997, *Facilitators, Mediators or Autonomous Agents*, Alexandru Ioan Cuza University, [online] Available: http://thor.info.uaic.ro/~amalia/courses/cws.pdf [Accessed : 14 January 2005].

Shoham, Y. 1997. ‘An Overview of Agent-oriented Programming’, In Bradshaw J. M. (ed.), *Software Agents,* AAAI Press, Menlo Park, Calif.

Siegel, P.H. & Mart, F. 1995, *A Comment on the Application of Grounded Theory to Accounting Research*, Baylor University, [online] Available : http://business.baylor.edu/Charles_Davis//lab/reporter/summer95/sigel.htm [Accessed: 16 October 2004].

Smith, B. & Tolman, T. 2000, ‘Can We Talk? Public Safety and the Interoperability’, *National Institute of Justice Journal*, April, pp.17-21, USA.

Smith, B. 2003, *Zigging and Zagging Into The Future*, REED BUSINESS INFORMATION [online] Available: http://www.wirelessweek.com [Accessed 11 November 2004].

Sobrado, I. 2001, ‘Evaluation of Two Security Schemes for Mobile Agents’,*ACM SIGCOMM Computer Communication Review*, Vol. 31, Issue 2 supplement.

Storey, M. Blair, G and Friday, A. 2002,‘MARE: Resource Discovery and Configuration in Ad Hoc Networks’, *Mobile Networks and Applications*, Issue 7, pp 377–387.

Strauss, A. & Corbin, J. 1990, *Basic qualitative research: Grounded theory procedures and techniques*, Newbury Park: Sage.

Struhsaker, P. 2003, *Including VoIP over WLAN in a Seamless Next-Generation Wireless Environment*, White Paper, Texas Instruments Incorporated. [online] Available: www.ti.com/wlan [Accessed 15 September 2005].

Sundsted, T. (1998), An introduction to agents. *Java World*, [Online] Available: http://www.javaworld.com/javaworld/jw-06-1998/jw-06-howto.html. [Accessed 9 December 2004].

Sycara, K. et al., 2003, The RETSINA MAS, a Case Study Software Engineering for Large-Scale Multi-Agent Systems: *Research Issues and Practical Applications*, Garcia, A., Lucena, C., Zambonelli, F., Omici, A., Castro, J. (eds.), Springer-Verlag, Berlin Heidelberg, Vol. LNCS 2603, July, pp. 232--250.

Symth, P. 2004, *Mobile and Wireless Communications: Key Technologies and Future Applications*, The Institution of Electrical Engineers, London, UK.

Tellis, W. 1997, ‘Introduction to case study’, *The Qualitative Report’*, Vol. 3, No. 2, [online] Available: http://www.nova.edu/ssss/QR/QR3-2/tellis1.html [Accessed 26 January 2005].

*The fall of the World Trade Center* 2002 video recording, BBC, U.K.

The US National Institute of Justice guide for the Selection of Communication Equipment for Emergency First Responders 2002, *Guide for the Selection of Personal Protective Equipment for Emergency First Responders, National Institute of Justice* [online], Available: http://www.ncjrs.org/pdffiles1/nij/191518.pdf [Accessed 15 December 2004].

Theil, S. 2001,'Love Those Wearables!', *Newsweek*, 4 September, Accessed 26 October 2004, [online] Available: http://www.keepmedia.com/pubs/Newsweek/2001/04/09/

Thiel, A. and Stambaugh, H. 2001, *United States Fire AdministrationTechnical Report Improving Firefighter Communications*, SPECIAL REPORT, [online] Available: http://www.usfa.fema.gov. [Accessed 11 November 2004].

US National Commission on the Terrorists Attack Upon the United States 2004, *The 9/11 Commission Report,* Special Report, Washington, USA.

US Public Safety Wireless Advisory Committee 1996, FINAL REPORT OF THE PUBLIC SAFETY WIRELESS ADVISORY COMMITTEE TO THE FEDERAL COMMUNICATIONS COMMISSION AND THE NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION, [online] Available: http://ntiacsd.ntia.doc.gov/pubsafe/publications/PSWAC_AL.PDF [Accessed 25 November 2004].

Vainio, A. 2000, *Bluetooth Security*, Helsinki University of Technology [online]. Available: http://www.niksula.cs.hut.fi/~iiitv/bluesec.html [Accessed 4 October 2003].

Vigna, G. (1997). Protecting Mobile Agents through Tracing. Proceeding *Third Workshop on Mobile Object Systems*. Jyväskylä, Finland, [online] , Available: http://citeseer.nj.nec.com/vigna97protecting.html [Accessed 2 October 2004].

Vitek, J. and Tschudin, C. (eds.) 1997, Mobile *Object Systems: Towards the Programmable Internet* , Springer Verlag, Heidelberg.

Waldrop, M. M. 2002, 'Can Sensemaking keep us safe', *TECHNOLOGY REVIEW*, March.

Walker, J. 2004, *Mesh Networks References*, Technical paper, Applied Wireless Local Area Network Inc., Viewed 23 December 2004, <http://www.wi-fitechnology.com/Wi-Fi_Reports_and_Papers /Mesh_Networks_References.html >

Wallenius K. 2004, 'Support for Situation Awareness in Command and Control', *Proceedings of the Seventh International Conference on Information Fusion*, Stockholm, Sweden.

Weick, K. E., Sutcliffe, K. M. Obstfeld, D. 2000, *ORGANIZING AND THE PROCESS OF SENSEMAKING*, [online] Available at: http://web.gsm.uci.edu/~dobstfel/Articles/Organizing%20and%20the%20Process%20of%20Sensemaking.pdf.

Wendelken, N., McGrath, S. P., and Blike, B. 2001, *AGENT BASED CASUALTY CARE – A MEDICAL EXPERT SYSTEM FOR MODERN TRIAGE*, Dartmouth University [online], Available : http://www.ists.dartmouth.edu/projects/frsensors/artemis/papers/abccare-suzanne.pdf [Accessed 13 September 2004]

*What is a literature review?* 2000, An interview with McKillap, S. , Central Queensland University [online] Available : http://www.library.cqu.edu.au/tutorials/litreviewpages/whatsm.htm [Accessed, 29 February 2005].

White, J. 1996, *Mobile Agents White Paper*, General Magic, USA.

White, J. 1996, *Mobile Agents White Paper*, General Magic, USA.

Whitehead, P. 2000, 'Mesh networks; a new architecture for broadband wireless access systems', *Proceeding of IEEE RAWCON2000*, pp.43-46.

*Why Wireless for Public Safety?* 2004,Wireless Ready Alliance, view November 2004, [online] Available: http://www.wirelessready.org/safety.asp [Accessed 12 January 2005].

Wooldridge, M. 2001, *An introduction to multiagent systems*, J. Wiley, New York.

Wooldridge, M. and Jennings, N. R. 1995, 'Intelligent Agents: Theory and Practice', *Knowledge Engineering Review*, October.

Yin, R. K. 2003, '*Case Study Research, Design and Methods'*, 3rd ed. Newbury Park, Sage.

Yufik Y. M. 2003, 'Transforming Data into Actionable knowledge in Network Centric Warfare', *Journal of Battlefield technology*, March, Vol 6, No 1.

Zachary, W., Le Mentec, J-C., and Ryder, J. 1996, 'Interface agents in complex systems, in Ntuen, C. A. and Parks, E. H. (eds.), *Human Interaction with Complex Systems: Conceptual Principles and Design Practice*, Kluwer

Academic Publishers Proceedings of the 33rd Hawaii International Conference on System Sciences.

Zasowski, T. et al., 2003,'UWB for Non–Invasive Wireless Body Area Networks: Channel Measurements and Results', *Proceeding of IEEE Conference on Ultra Wideband Systems and Technologies,* Reston, Virginia, USA.

ZigBee Alliance 2004, *Emerging Standards: Where do ZigBee/UWB fit*, White Paper, ZigBee Alliance. [online] Available: http://www.ZigBee.org [Accessed: 17 September 2004].

Zikmund W. G., 2000, *Business Research Methods*, Sixth Edition, The Dryden Press, USA

Zyren, J. and Petrick, A. 2004, *IEEE 802.11 Tutorial*, YDI Wireless, [online] Available: http://www.ydi.com/deployinfo/wp-80211-tutorial.php [Accessed 26 January 2005 ].

Article below removed due to Copyright reasons

Nosek, John T. "Collaborative Sensemaking Support: Progressing from Portals and Tools to Collaboration Envelopes." *IJEC* 1.2 (2005): 25-39.